



Progressive Scan CCD Caméra réseau

Instructions d’installation

V1.2





TV7220 - TV7223

Préface

Chère cliente, cher client,

Nous vous remercions d'avoir porté votre choix sur cette caméra réseau de la série Eyseo proposée par la société ABUS Security-Center. Par l'achat de ce produit, vous disposez maintenant d'un appareil faisant appel à une technologie de pointe.

Ce produit est conforme aux exigences des directives européennes et nationales en vigueur. La conformité de ce produit a été prouvée. Les déclarations et documents correspondants ont été déposés chez le fabricant.

Pour que cette conformité persiste et qu'un fonctionnement en toute sécurité puisse être assuré, lire attentivement ces instructions de service ! Pour de plus amples renseignements, veuillez vous adresser à votre vendeur spécialiste sur site.

Cette caméra réseau sert à la surveillance d'objets. Dans ce cadre, les signaux vidéo enregistrés sont transmis sous forme numérique à un ordinateur en réseau. Le logiciel installé sur l'ordinateur permet l'enregistrement simultané d'un total de 16 signaux vidéo connectés. L'enregistrement de données est soumis à la réglementation sur la protection des données en vigueur dans le pays correspondant. Le logiciel Internet Explorer permet d'obtenir un accès mondial aux caméras installées (protégées par mot de passe).

Consignes de sécurité

Eviter à tout prix que la caméra réseau et les composants qui y sont reliés entrent en contact avec l'humidité, par exemple, dans un sous-sol ou autre. Une utilisation de ce produit autre que celle décrite précédemment risque d'endommager l'appareil. De plus, une utilisation non conforme expose à des risques de court-circuit, d'incendie et de choc électrique, etc. L'appareil est homologué pour un branchement à une alimentation de classe 2 de 12 volts de tension continue. La modification, la transformation ou l'ouverture de la structure d'une quelconque partie de ce produit n'est pas autorisée. Son raccordement au réseau électrique public doit avoir lieu dans le respect des réglementations en vigueur dans le pays correspondant. S'informer au préalable.

Pour éviter les incendies et les blessures, tenir compte des consignes ci-dessous :

Fixer solidement l'appareil à un endroit sec à l'intérieur.
Veiller à ce que la ventilation soit suffisante.
Ne pas exposer l'appareil à des températures inférieures à 0°C ou supérieures à 35°C.
L'appareil a été conçu pour être utilisé uniquement à l'intérieur.
L'humidité maximale ne doit pas dépasser 90 % (sans condensation).
Ne réaliser tous les travaux sur l'appareil qu'après l'avoir mis hors tension.

Prendre les mesures de précaution ci-dessous pour que l'appareil fonctionne parfaitement :

La caméra réseau est alimentée par un bloc d'alimentation en courant continu de 12V.
Le branchement du bloc d'alimentation aux 230 V c.a. du secteur doit être réalisé par le biais d'une ligne séparée protégée contre les courts-circuits.
Les travaux de branchement au secteur sont soumis à la réglementation en vigueur dans le pays correspondant.

Généralités :

Des travaux d'installation non conformes et incorrects risquent d’être à l’origine de perturbations et d'une mauvaise qualité d'image. Lire donc attentivement l'intégralité de la présente notice et tenir compte lors de l'installation du système de la désignation exacte des câbles et des composants utilisés.

Sous réserve en tout temps de modifications techniques.

Préalablement à la mise en service du produit

Il se peut que la mise en service de systèmes de surveillance soit interdite par la loi dans certains pays. Cette caméra réseau est non seulement une caméra puissante conçue pour fonctionner sur le Web, mais elle peut également être intégrée à un système de surveillance flexible. Préalablement à la mise en service du système, l'utilisateur est tenu de s'assurer que la surveillance a lieu dans le respect des dispositions légales applicables.

Avant d'installer le produit, vérifier que rien ne manque (page 5 : Livraison). Tenir compte des consignes figurant dans les instructions d'installation, avant d'installer la caméra réseau . Lire attentivement le chapitre « Installation » et suivre les instructions qu'il contient, en vue d'éviter une détérioration liée à un mauvais assemblage ou une installation incorrecte. Ceci permet d'assurer une mise en service conforme de l'appareil permettant de l'utiliser aux fins auxquelles il a été prévu.

Les annexes A et B proposent d'éventuelles solutions permettant d'éliminer les erreurs les plus fréquentes, lors de l'installation et de la configuration.
Les instructions d'installation décrivent les possibilités d'utilisation les plus diverses de la caméra réseau .

Les paragraphes munis du symbole ⚠ signalent à l'utilisateur la présence d'informations particulièrement importantes. La non-observation de ces remarques risque d'entraîner un endommagement de l'appareil ou des préjudices corporels.

Table des matières

Livraison

Caméra réseau
TV7220/TV7221/TV7222/TV7223



Objectif



Antenne (SEULEMENT TV7221/23)



Adaptateur secteur



Pied de caméra



CD logiciel



Instructions d’installation (sur CD)

Installation matérielle



S’assurer que tous les accessoires et les articles listés ci-dessus fassent partie de la livraison. Suivant l’utilisation faite du produit, il se peut qu’un câble Ethernet soit nécessaire. Ce dernier doit être conforme aux spécifications de la catégorie UTP 5 (CAT 5) et ne doit pas faire plus de 100 mètres de long.

En vue d’éviter tout risque de choc électrique, brancher d'abord la prise femelle de l'adaptateur secteur à la caméra réseau, avant d’enficher l’adaptateur secteur dans la prise murale.

 Pour une installation correcte des périphériques, contactez votre revendeur.

Instalation en ethernet

Le caméra de réseau CCD scan progressif essaye comme premier d'interpeler l'Ethernet par fil. Si elle ne peut pas atteindre cela, la caméra essaye d'atteindre plus loin le réseau sans fil (W-LAN).

En la mise sous tension, ce LED sur l'avant allume rouge, et la procédure d’initialisation commence ensuite. Pendant l'attribution d'adresse IP le LED s’allume vert. Si ce processus est achevé, le DED s'enflamme vert dans une synchronisation d’une seconde. Des indications trouvent au dépannage vous dans l'annexe.

Installation Ethernet

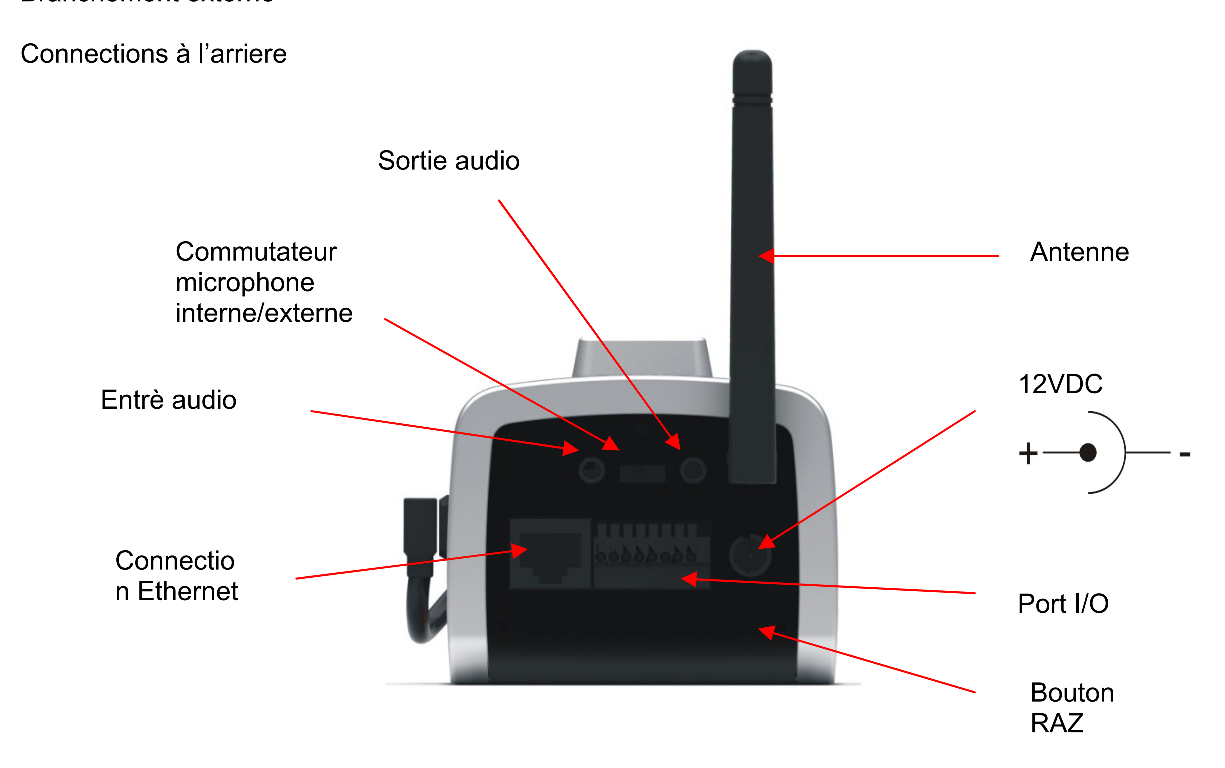
S’assurer que la caméra est directement liée au PC par le biais d’un câble (cross-link-câble) ou liée au réseau par le biais d’un commutateur/moyeu. Brancher le transformateur de la caméra au réseau du secteur la DEL bleu de la caméra s’allume si le branchement au réseau est correctement fait .
Si il n’y a pas de réseau, la caméra enclenche sur le mode –WLAN.

Installation WLAN

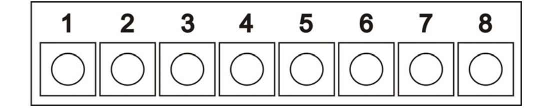
Si la caméra est alimentée et ne trouve pas de réseau Ethernet, elle enclenche au mode WLAN et cherche une station d’accès (Acces point) avec la désignation «default ». Cette désignation sera désignée comme SSID (service set identifier). La DEL sur la face avant s’allume en bleu si la station d’accès est trouvée.
Si la connexion avec le réglage n’est pas effectuée avec succès, reliez la caméra par le biais d’un câble au réseau et refaite la configuration.

Branchement externe

Connections à l'arriere

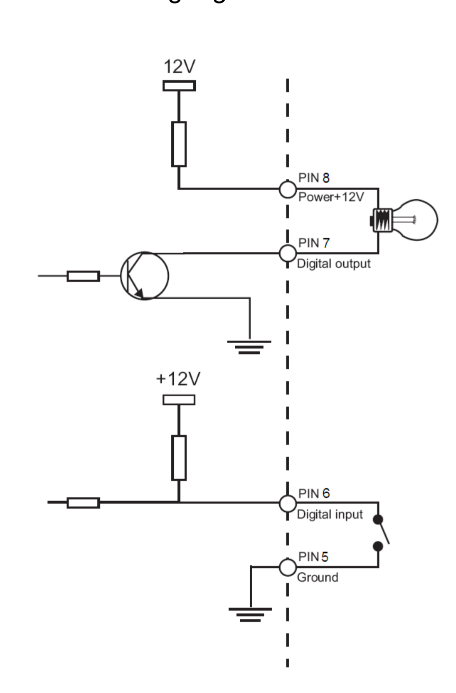


Sortie / entrè de commutation



1 : pas utilisé
2 : pas utilisé
3 : pas utilisé
4 : pas utilisé
5 : GND
6 : entrè de commutation
7 : sortie de commutation
8 : Allimentation 12VDC

Schaltein-/ausgang



Premier accès à la camera

Le premier accès au serveur vidéo se fait en utilisant l'assistant d'installation 2.
Après avoir démarré l'assistant il détecte les caméras réseau Eyseo et les serveurs vidéo branchés sur votre réseau.

L'adresse IP standard du serveur vidéo est la suivante: **169.254.0.99**.
Si un serveur DHCP est disponible sur le réseau, l'attribution de l'adresse IP se fera automatiquement en tenant compte de votre configuration de réseau.

Vous pouvez modifier les données du réseau comme l'adresse IP ou la masque de sous-réseau [Configuration du système / Réseau], et ainsi adapter votre réseau de destination (ex. IP=192.168.0.99 / masque de sous-réseau = 255.255.255.0).

Pour créer une connexion au serveur vidéo cliquez deux fois sur l'objet souhaité dans la liste.



Après avoir lancé l'assistant d'installation 2 celui-ci ajoutera possiblement une adresse IP virtuelle aux réglages de réseau actuels. Ceci dépend, si un DHCP est activé dans votre réseau. Après l'achèvement de l'assistant d'installation 2 cette adresse IP virtuelle est à nouveau éloignée.

Grâce à cette adresse IP virtuelle la première configuration du serveur vidéo est rendue très facile. Ainsi une configuration manuelle de l'adresse IP de l'adaptateur réseau du PC n'est plus nécessaire.

Accès à la caméra réseau par le biais d'Internet Explorer

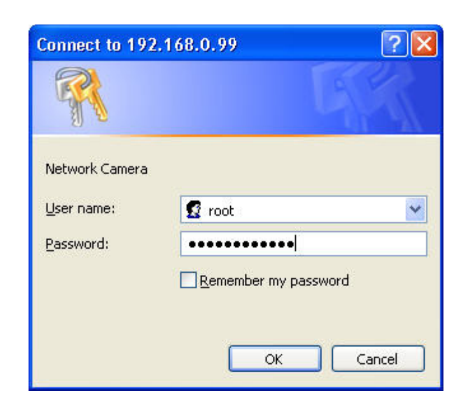
Définition d'un mot de passe évitant un accès non autorisé

La caméra réseau n'a pas de mot de passe administrateur.
Pour des raisons de sécurité, l'administrateur doit immédiatement définir un nouveau mot de passe. A l'issue de l'enregistrement d'un tel mot de passe administrateur, la caméra réseau invite à entrer le nom d'utilisateur et le mot de passe, préalablement à tout accès. L'administrateur peut définir vingt (20) comptes utilisateurs au total. Chaque utilisateur dispose d'un accès à la caméra réseau, mais il ne peut pas accéder à la configuration système. Quelques fonctions système critiques, telles que la configuration système, la gestion des utilisateurs et la mise à jour des versions de logiciels sont réservées à l'administrateur. Le nom d'utilisateur de l'administrateur est toujours « root » et il ne peut pas être modifié. A l'issue de la modification du mot de passe, le navigateur affiche une fenêtre d'authentification et invite à entrer le nouveau mot de passe. A l'issue de la définition du mot de passe, une récupération du mot de passe administrateur n'est pas possible. La seule possibilité consiste à rétablir la configuration d'origine.

Pour entrer le mot de passe :

Exécutez Internet Explorer et entrez l'adresse IP de la caméra (par ex. : <http://192.168.0.99>)

Une boîte de dialogue d'authentification apparaît.

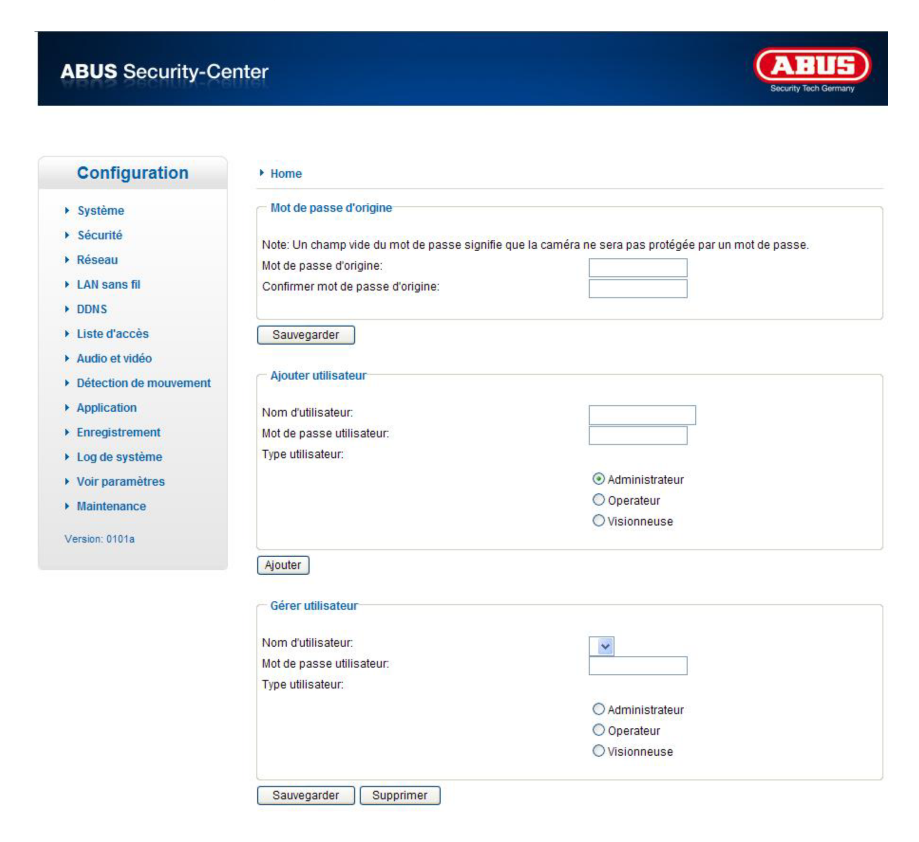


➔ La connexion à la caméra réseau est ensuite établie et le système visualise une séquence vidéo.

⚠ Remarque : les paramètres de sécurité définis sur votre PC risquent d'empêcher une séquence vidéo. Modifiez les paramètres concernés en cliquant sur « Outils/Options Internet/Sécurité », puis en réduisant le niveau de sécurité. Veillez notamment à activer les commandes Active X et les téléchargements.

Modification du mot de passe administrateur

Cliquez sur « **Configuration**« , puis sur « **Sécurité**« .



Entrez le mot de passe de l'administrateur dans le champ « **Mot de passe d'origine**« et confirmez-le dans le champ « **Confirmer mot de passe d'origine** ».

Cliquez sur « **Sauvegarder** ».
Le système enregistre le nouveau mot de passe administrateur.

Cliquez sur « **HOME** » dans la barre gauche pour quitter la configuration.

Installation du plug-in

Lors du premier accès à la caméra réseau sous Windows, le navigateur Internet invite, le cas échéant, à installer un nouveau plug-in pour cette dernière. Cette invitation dépend des paramètres de sécurité Internet définis pour le PC de l'utilisateur. Si le niveau de sécurité le plus élevé a été défini, l'ordinateur risque de refuser toute installation ou toute tentative d'exécution. Ce plug-in permet un affichage vidéo dans le navigateur. Un clic sur « **Oui** » permet de continuer. Si le navigateur Internet refuse de poursuivre l'installation, ouvrez les paramètres de sécurité Internet et réduisez le niveau de sécurité ou contactez l'administrateur IT ou réseau.



Droits de l’administrateur

Ecran « Network camera »

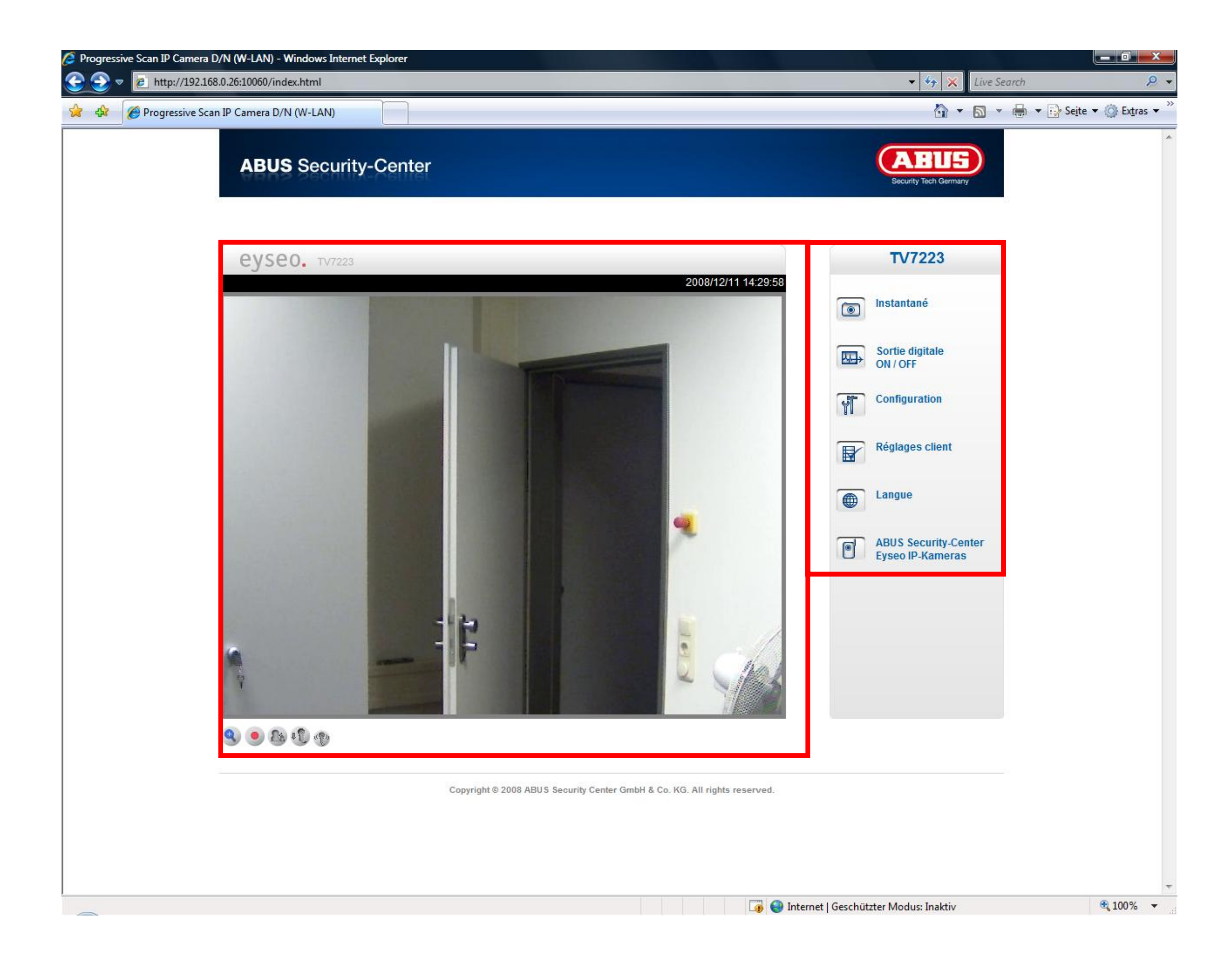
La fenêtre principale affichée est en deux parties :

« **Configuration** » : Ces éléments d'interface utilisateur permettent de configurer la caméra.
« **Zone d’affichage des données d’image de la caméra** »: séquence vidéo de la caméra

Un clic sur le lien « **Configuration** » à gauche de la zone d’affichage de l’image permet de passer à l'écran de configuration.

Sortie Digitql: Ici, la sortie de la caméra de réseau peut être enclenchée manuellement

Enregistrement locale : Un enregistrement peut être commencée ou arrêtée sur le disque dur local. L’enregistrement est configurée sous „Configuration client/MP4 options d’enregistrement «



Zoom numérique et enregistrement instantané

Cliquez sur l’icône représentant une loupe sous la zone d’affichage de l’image. Le système affiche ensuite les boutons de commande du zoom numérique. Désactivez la case « **Disable digital zoom** » et modifiez le facteur de zoom à l’aide de la réglette.

« **Snapshot** » (Instantané)

Faites un clic sur « **Instantané** ». Le navigateur Internet affiche une fenêtre séparée présentant l’instantané. Pour enregistrer, faites un clic gauche sur l’image de l’instantané, puis utilisez l'icône représentant une disquette ou utilisez la fonction d'enregistrement à l'issue d'un clic droit.



« Client Settings » (Configuration client)

Au premier affichage de l'écran « **Client settings** » sous Windows, le navigateur Internet invite à installer un nouveau plug-in. Ce plug-in a été enregistré à des fins de certification et peut permettre de modifier les paramètres de l'écran « **Client Settings** » coté client. Un clic sur « **Oui** » installe le plug-in. Si le navigateur Internet refuse de poursuivre l'installation, ouvrez les paramètres de sécurité Internet et réduisez le niveau de sécurité ou contactez l'administrateur IT ou réseau.



L'écran « **Client Settings** » prévoit deux paramètres à définir : La zone « **Media options** » permet à l'utilisateur de désactiver la fonction audio ou vidéo. La zone « **Protocol options** » permet de sélectionner un protocole de liaison entre le client et le serveur. Deux protocoles au choix visant à optimiser l'application sont disponibles : UDP,TCP et HTTP.

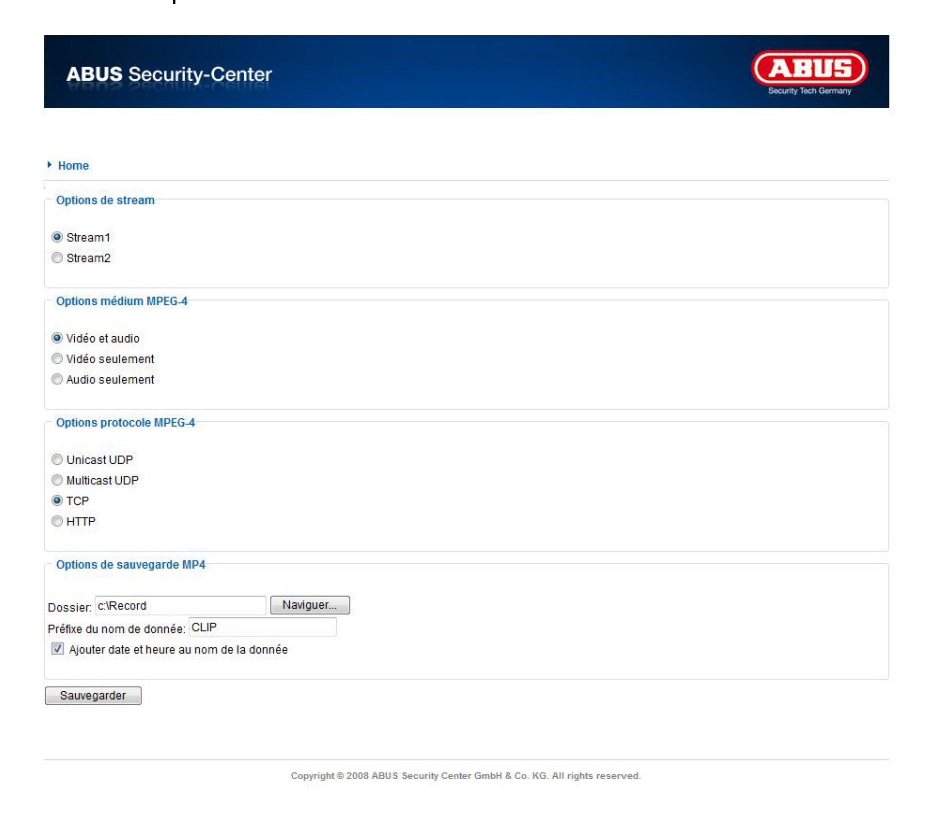
Le protocole UDP permet un nombre plus élevé de séquences audio et vidéo en temps réel. Cependant, certains paquets de données risquent d'être perdus lors d'un trafic important sur le réseau. De ce fait, des images visualisées risquent d'être moins nettes. Le protocole UDP est recommandé en l'absence d'exigences particulières.

Dans le cadre du protocole TCP, seul un nombre réduit de paquets de données sont perdus. Ce protocole assure donc un affichage net. Cependant, le désavantage de ce protocole réside dans le fait que la séquence en temps réel est de moins bonne qualité que celle du protocole UDP.

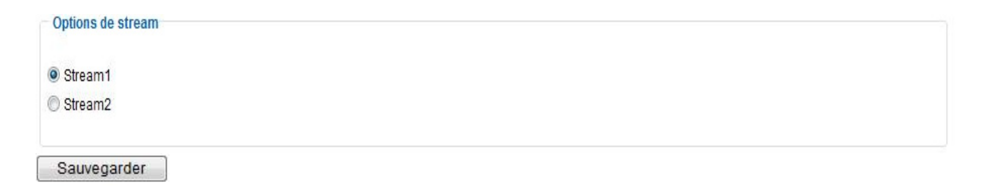
Vous choisissez le HTTP-Protocol, si le réseau est protégé par un Firewall et seulement le HTTP-Port (80) peut être ouvert. Dans ce mode, aucun audio n'est envoyé.

L'ordre recommandé de sélection du client est normalement le suivant : UDP – TCP – HTTP. A l'issue de la réussite du branchement de la caméra réseau , la zone « **Protocol options** » affiche le protocole sélectionné. Le protocole sélectionné est enregistré sur le PC de l'utilisateur et utilisé pour la connexion suivante. A l'issue de l'apport d'une modification à l'environnement réseau ou si l'utilisateur souhaite que le navigateur Internet détecte de nouveau la caméra réseau , sélectionnez au clavier le protocole UDP, enregistrez la sélection, puis basculez de nouveau dans « **HOME** » , pour rétablir la connexion.

Internet Explorer



Mozilla Firefox:

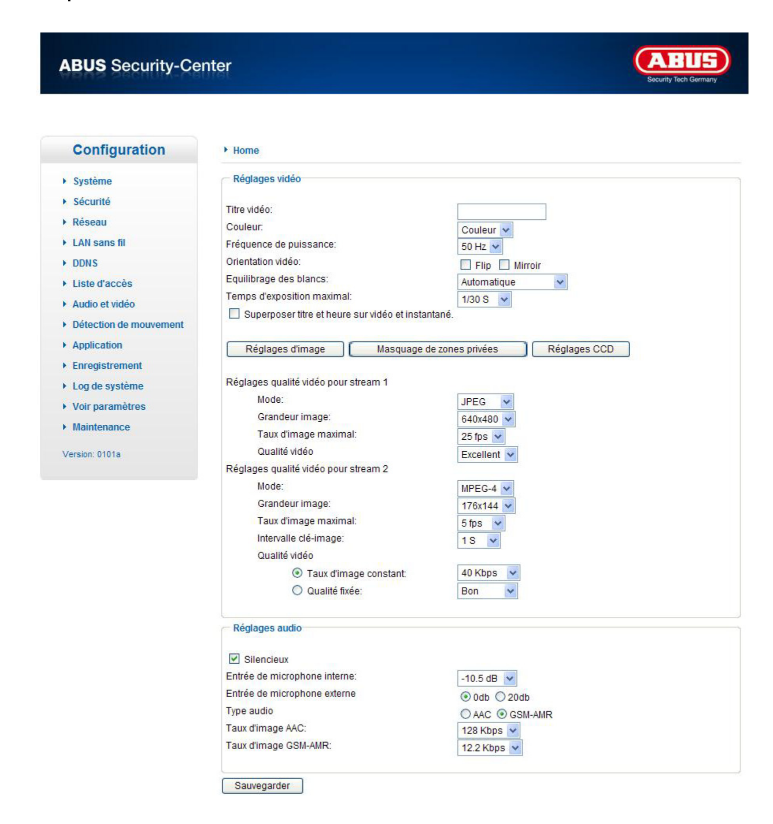


<url> *http://<Network Camera>/protocol.html*
« Network Camera » est l'adresse IP par défaut ou le nom d'hôte de la caméra réseau .

Paramètres Administrateur

« Configuration / Audio et vidéo»

La meilleure performance est obtenue avec une fréquence d'images élevée, un rendu vidéo de très bonne qualité et une bande passante réseau la plus faible possible. Les trois facteurs « **Taux d'image maximal** », « **Taux d'image constant** » et « **Qualité fixée** » sur l'écran Configuration vidéo dépendent les uns des autres.



Accès mobile à la caméra réseau

De nombreux téléphones portables modernes prennent en charge un accès à des séquences vidéo MPEG4 et des données audio GSM-AMR. La bande passante limitée ne permet que la gestion d'une résolution maximale de 176 x 144 pixels.

Pour une fréquence d'images élevée

La bande passante réseau doit être assez importante pour permettre d'obtenir un bon effet visuel en temps réel (plus de 20 images par seconde). Si la bande passante réseau est supérieure à 1 Mbps, il convient de régler la valeur de « **Taux d'image constant** » sur 1000 Kbps ou 1200 Kbps et celle de « **Qualité fixée** » sur la qualité maximale. La fréquence d'images maximale est de 25 images par seconde pour un système PAL et de 30 pour un système NTSC. Si la bande passante réseau dépasse 384 Kbps, le débit peut être défini en fonction de la bande passante et la fréquence d'images mise sur 25 ou 30 fps (images par seconde). En cas de modification radicale des images dans l'environnement concerné, la fréquence d'images peut être réduite à 20 images par seconde, afin de définir un débit plus faible. Il en résulte une amélioration de la qualité vidéo, sans que la différence entre 20, 25 ou 30 images par seconde ne soit visible à l'œil nu. Si la bande passante réseau est inférieure à 384 Kbps, définissez le débit « **Taux d'image constant** » en fonction de la bande passante et essayez d'obtenir la meilleure performance par un ajustement du taux « **Taux d'image maximal** ». Dans un réseau plus lent, une fréquence d'images plus élevée est à l'origine d'un rendu moins net et d'une distorsion de l'image Une autre solution permettant obtenir une meilleure qualité d'image consiste à sélectionner « **176x144** » au niveau de l'option Size ou « **320x240** » pour un agrandissement de l'image. La performance en matière de qualité vidéo varie suivant le nombre d'utilisateurs ayant ouvert une session réseau. Une liaison de mauvaise qualité et une limitation du nombre des rafales réseau risquent d'altérer la performance.

Pour des images haute qualité

En vue d'obtenir la meilleure qualité vidéo, mettez l'option « **Qualité fixée** » sur « **Detailled** » ou sur « **Excellent** » et réglez le taux « **Max frame rate**« de manière à ce que ce taux corresponde à la bande passante du réseau. Si le réseau devait être lent et que vous obtenez des fractions d'images, passez au protocole TCP, sur l'écran « **Client settings** » et sélectionnez le mode de transmission adéquat. Un temps de retard lié à la lenteur du réseau risque d'altérer les images. Plus le nombre d'utilisateurs ayant ouvert une session réseau est élevé, plus ce retard est long.

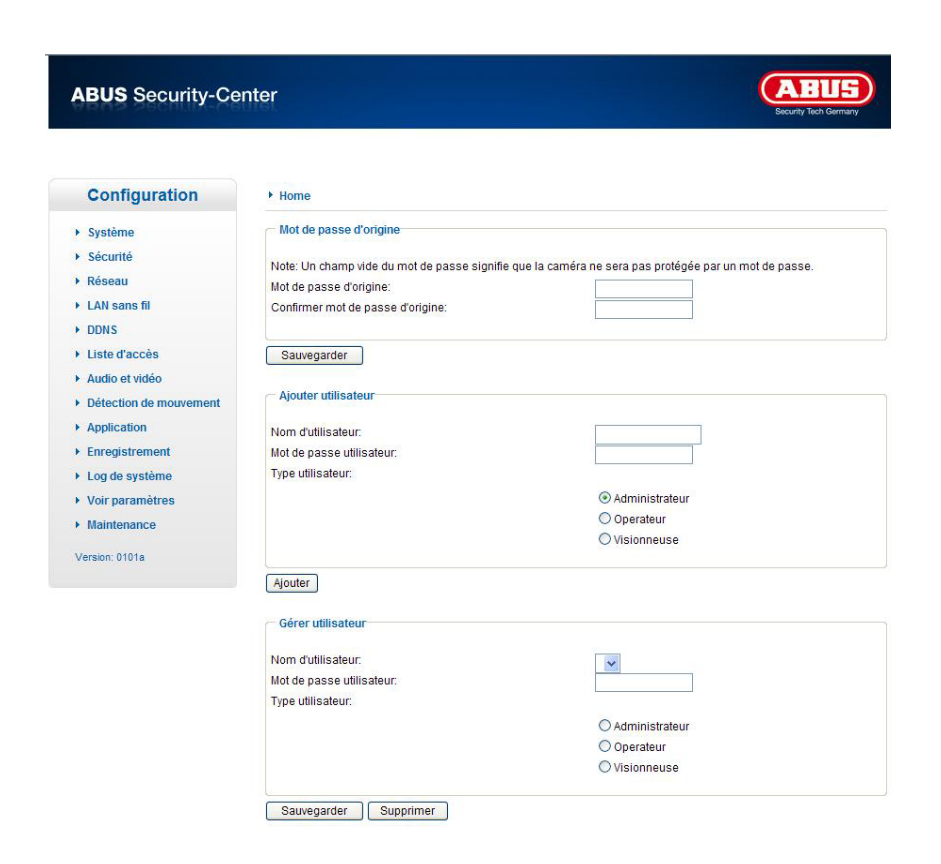
Pour une fréquence d'images élevée et des images haute qualité

En présence d'un réseau large bande, mettez l'option « **Taux d'image constant** » sur « **512Kbps**« ou plus sans modifier la valeur définie pour l'option « **Taux d'image constant** ». La bande passante peut également être définie en fonction de la vitesse effective du réseau ou de la fréquence d'images. Commencez par 30 images par seconde et réduisez cette valeur en vue d'obtenir la meilleure performance. Cependant, ne pas définir moins de 15 images par seconde. En l'absence d'une amélioration de l'image, sélectionnez la valeur la plus faible pour l'option « **Taux d'image constant** ».

Protection par mot de passe de la caméra réseau

Mot de passe d'origine de « root »

La caméra réseau est livrée sans mot de passe. Dans ces conditions, un accès à la caméra réseau et à la configuration est possible pour tous, dans la mesure où l'adresse IP est connue. L'affectation d'un mot de passe à la caméra est impératif , si la caméra réseau doit être accessible à d'autres utilisateurs. Entrez un mot de passe pour activer la protection



Création de comptes de nouveaux utilisateurs

Dans « **Configuration** » sélectionnez l'option de menu « **Sécurité** » . Utilisez à présent la zone « **Ajouter utilisateur** ».

Ajoutez un compte avec nom d'utilisateur et mot de passe pour les autre utilisateurs. La caméra réseau permet de créer vingt comptes utilisateurs. Dans ce cadre, la caméra ne fait que vérifier l'autorisation d'accès du nom d'utilisateur et du mot de passe concernés. Ceci permet une utilisation commune à divers niveaux d'un même compte par plusieurs utilisateurs.

Construction d'une application de surveillance

L'administrateur peut utiliser le détecteur de mouvement intégré .surveiller le changement des images et les signaler. En plus les enregistrements instantanés des événements peuvent être transmis à une adresse
E-mail ou à un serveur FTP.
Les réglages dans le menu de configuration « **Réseau** », « **Détection de mouvement** » et « **Application** » sont nécessaires. Vous trouverez des amples informations sur la page « configuration du système »

Mise à jour du logiciel

L'utilisateur peut télécharger la version actuelle à partir du site Internet www.abus-sc.com .
Un assistant Mise à jour convivial est disponible pour la mise à jour du logiciel de la caméra réseau (Installation Wizard / Upgrade). L'exécution de la fonction de mise à jour est réservée à l'administrateur. Pour actualiser le système :

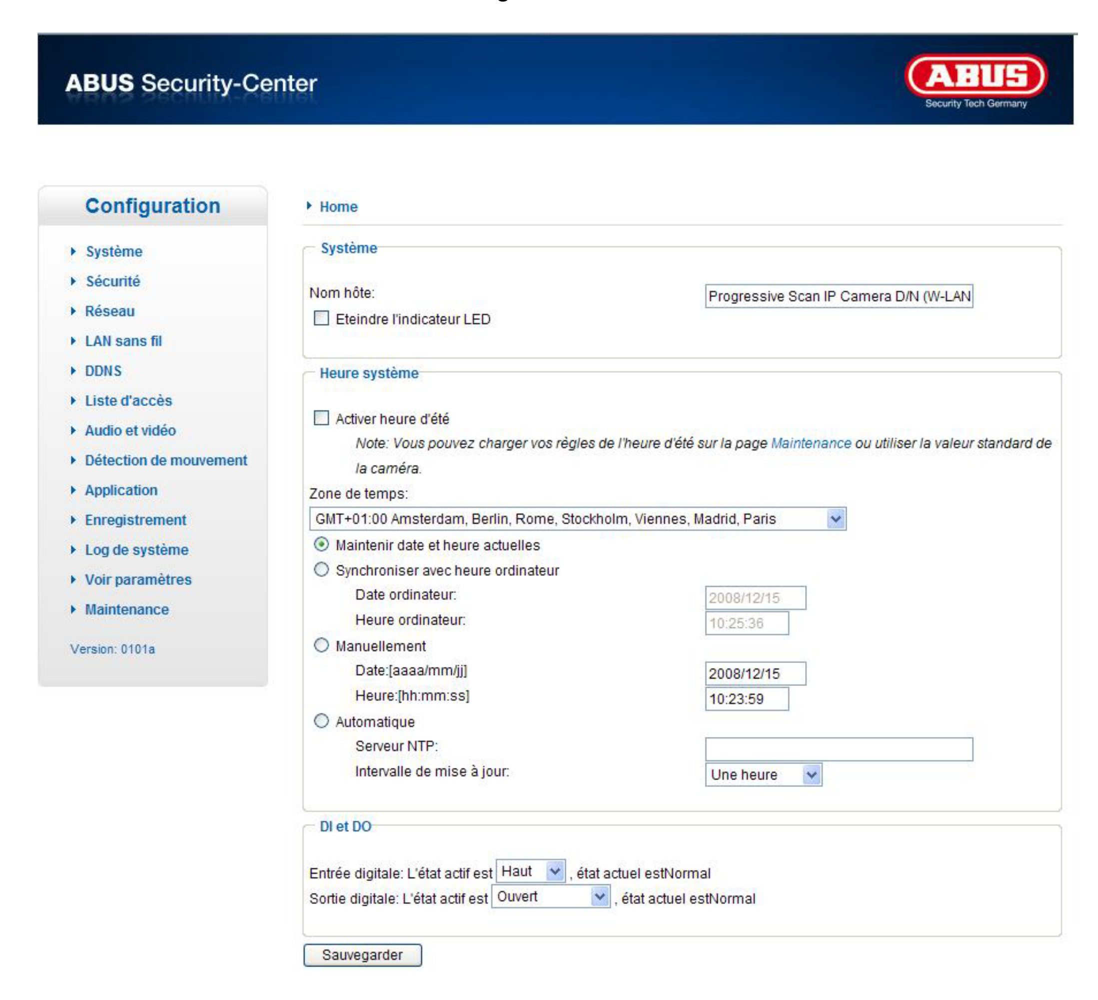
1. Chargez le fichier de microprogramme nommé xxx.pkg disponible dans le répertoire produits correspondant.
2. Démarrez l'assistant Mise à jour et suivre les instructions.
3. L'opération se termine en quelques minutes, puis le système redémarre automatiquement.

La mise à jour du logiciel est aussi possible sur le menu „Configuration / Maintenance ».

Une coupure de courant pendant l'opération d'écriture de la mémoire Flash risque d'endommager irréversiblement le programme disponible dans la mémoire de la caméra réseau. Si un démarrage de cette dernière s'avère être impossible à l'issue de la mise à jour, contactez le support technique de votre revendeur.

Configuration du système

L'accès à la configuration du système est réservé à l'administrateur. Les pages suivantes décrivent chacune des catégories de la barre gauche. Les termes en caractères gras sont des termes affichés sur les écrans d'options. L'URL disponible sous l'illustration ci-dessous permet à l'administrateur d'atteindre directement l'écran de configuration.



« url » *http://"Network Camera"/setup/config.html*
« Network Camera » est le nom de domaine ou l'adresse IP par défaut de la caméra réseau .

« url » *http://"Network Camera"/setup/system.html*
« Network Camera » est le nom de domaine ou l'adresse IP par défaut de la caméra réseau .

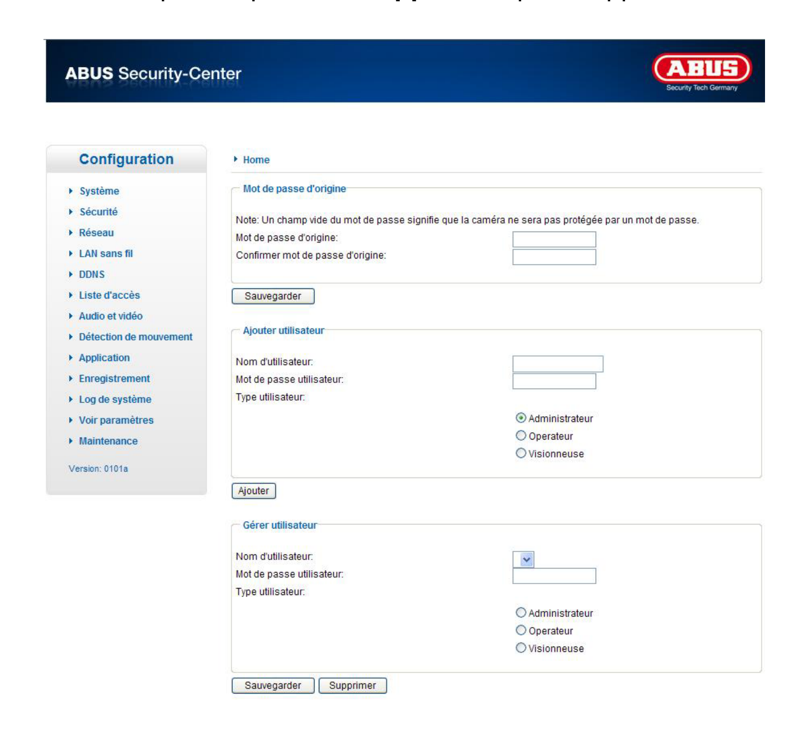
Ecran « System »

„**Nom hôte**“ ce champ affiche le titre de la fenêtre principale.
„**Eteindre l’indicateur LED**“ L’activation de cette option permet de désactiver l’affichage à DEL sur la face avant de la caméra. Ceci permet d’éviter que des tiers puissent remarquer que la caméra est en cours de fonctionnement.
„**Maintenir date et heure actuelles**» Sélectionnez cette option pour enregistrer la date et l’heure actuelle de la caméra réseau . Une horloge temps réel interne permet de retenir la date et l’heure même à l’issue de l’arrêt du système.
„**Synchroniser avec heure ordinateur**“ Cette option synchronise la date et l’heure de la caméra réseau avec celles de l’ordinateur local. La date et l’heure en lecture seule du PC sont affichées à l’issue de leur mise à jour.
„**Manuellement**“ Cette option règle la date et l’heure suivant les données saisies par l'administrateur. Tenez compte du format lors de la saisie dans le champ correspondant.
„**Automatique**“ Cette option synchronise via l’Internet la date et l’heure avec celle du serveur NTP, au démarrage de la caméra réseau . Cette synchronisation n'est possible que si le serveur horaire affecté est joignable.
„**Serveur NTP**“ Ce champ permet d’affecter l’adresse IP ou le nom de domaine du serveur horaire. Si ce champ reste vide, la caméra réseau est connectée aux serveurs horaires par défaut.
„**Zone de temps**“ cette zone de liste définit l’heure en fonction du serveur horaire pour la configuration locale.

Ne pas oublier de cliquer sur « **Sauvegarder** » pour que les modifications apportées deviennent effectives. Dans le cas contraire, une synchronisation de la date et de l'heure n'est pas exécutée.

Ecran « Security »

„**Root password**“ Permet de modifier le mot de passe de l’administrateur par la saisie d'un nouveau mot de passe. Pour des raisons de sécurité, la saisie de mots de passe est aveugle. A l’issue d’un clic sur « **Sauvegarder** », le navigateur Internet invite l’administrateur à entrer le nouveau mot de passe d’accès à la caméra réseau.
„ **Ajouter utilisateur**“ Entrez le nouveau nom d’utilisateur et le mot de passe correspondant, puis cliquez sur „ **Ajouter**“ . Le nouvel utilisateur apparaît sur la liste des noms d’utilisateurs. Vingt comptes utilisateurs peuvent être définis au total.
„**Gérer utilisateur**“ Cliquez sur la zone de liste des noms d'utilisateurs, recherchez l'utilisateur concerné, puis cliquez sur „**Supprimer**“, pour supprimer ce dernier de la liste.



« url » *http://“Network Camera“/setup/config.html*
« Network Camera » est le nom de domaine ou l’adresse IP par défaut de la caméra réseau .

Ecran « Network »

Toutes les modifications apportées sur cet écran entraînent un redémarrage du système, afin que les modifications apportées deviennent effectives. Vérifiez d’avoir complété correctement les champs correspondants, avant de cliquer sur « **Sauvegarder** ».

Connexion – réseau (Network)

« **LAN** » la connexion est LAN. Utiliser ce paramètre quand la caméra est reliée à une LAN »
Les paramètres adresse IP et subnet mask sont nécessaires.
« **PPPoE** » Utiliser ce paramètre quand la caméra est directement reliée à un modem DSL »
Vous recevrez le mot de passe et le nom d’utilisateur de votre ISP (internet service provider).

« **Obtenir adresse IP automatiquement**» après avoir redémarré la caméra réseau, elle obtient automatiquement une nouvelle adresse IP.

«**Utiliser adresse IP fixe** » les donnés du network par exemple adresse IP seront définies ici :

„**Adresse IP** “ L’adresse IP est nécessaire à l’identification réseau.
„**Masquage de sous-réseau**“ Elle permet de déterminer si la cible se trouve dans le même sous-réseau. La valeur par défaut est « 255.255.255.0 ».
„**Routeur standard**“ Il s’agit de la passerelle permettant la transmission d'images à un autre sous-réseau. Une configuration de routeur incorrecte empêche la transmission à ces destinataires situés dans des sous-réseaux différents. Pour une connexion avec un câble cross-link, donnez s.v.p absolument l`adresse IP de la caméra dans le même domaine que le subnet.
„**DNS primaire**“ Serveur du nom de domaine primaire permettant de convertir les noms d’hôtes en adresses IP.
„**DNS secondaire**“ Serveur du nom de domaine secondaire permettant de créer une copie de sauvegarde des DNS primaires.

« **Activer présentation UPnP** » le plug and play universel sera activé. C’est un élargissement du standard PnP sur l’environnement du network.
« **Activer transmission par port UPnP** » le plug and play universel de port de transmission du service réseau sera activé.

« PPPoE » : si la camera est exploitée dans ce mode , dans ce cas donnez les données suivantes de votre ISP(Internet Service Providers) : code d’utilisateur, mot de passe, confirmation de mot de passe.

HTTP:

« «**HTTP Port** « Ce port ne doit pas être obligatoirement le port par défaut 80 (80; 1025 ~ 65535). A l'issue de la modification du port, il convient d'informer l'utilisateur de la modification apportée, afin de permettre l'établissement d'une connexion. Exemple : si l’administrateur modifie le port HTTP de la caméra réseau , ayant 192.168.0.99 comme adresse IP, pour le faire passer de 80 à 8080, l’utilisateur doit entrer « http://192.168.0.99:8080 » au lieu de « http://192.168.0.99 » au niveau du navigateur Internet

„**Port http secondaire**“ HTTP Port für Stream 2
„**Nom d’accès pour stream 1**“ Zugangsname für den MJPEG Stream 1
„**Nom d’accès pour stream 2**“ Zugangsname für den MJPEG Stream 2

FTP:

„**Port FTP**“ Dies ist der interne FTP-Server-Port. Dies kann ein anderer Port als der vorgegebene Port 21 sein (21, oder 1025 - 65535).

Transmission RTSP (RTSP streaming)

„**Authentification**“ L’authentification peut être désactivée (standard) ou se trouver dans le mode simple ou élargie.

Si celle-ci est activée, un nom d’utilisateur et un mot de passe d’un utilisateur valable doivent être introduits lors de la création de la connexion RTSP (ex. administrateur).
ATTENTION: L’authentification RTSP doit être supportée par le lecteur vidéo (ex. Realplayer 10.5).

„**Nom d’accès pour stream 1**“ Le nom d’accès 1 sert pour créer une connexion d’un client. Le type Codec doit être MPEG4! Utilisez
rtsp://<IP-Adresse>:RTSP-port /<Zugangsname 1> pour créer une connexion.

„**Nom d’accès pour stream 2**“ Le nom d’accès 2 sert pour créer une connexion d’un client. Le type Codec doit être MPEG4! Utilisez
rtsp://<IP-Adresse>:RTSP-port /<Zugangsname 2> pour créer une connexion.

„**Port RTSP**“ Ce port peut différer du port 554 (554; ou 1025 à 65535). Veillez au format et au port HTTP lors de la modification.

„**Port RTP pour vidéo**“ Ce port peut différer du port 5558. Ce numéro de port doit être un chiffre paire.

„**Port RTCP pour vidéo**“ Ce port doit être le „Port RTP pour vidéo“ plus 1.

„**Port RTP pour audio**“ Ce port peut différer du port 5556. Le numéro de port doit être un chiffre paire.

„**Port RTCP pour audio**“ Ce port doit être le „Port RTP pour audio“ plus 1.

Multicast: Ces réglages peuvent être configurés pour stream 1 et 2.

„**Toujours Multicast**“ Activation pour toujours utiliser Multicast.

“**Adresse de groupe Multicast**” Spécifie un groupe d’hôtes IP faisant partie de ce groupe

“**Port vidéo Multicast**” Ce port peut différer du port 5560. Le numéro de port doit être un chiffre paire.

“**Port vidéo Multicast RTCP** ” Ce port doit être „Port vidéo Multicast“ plus 1.

“**Port audio Multicast**” Ce port peut différer du port 5562. Le numéro de port doit être un chiffre paire.

“**Port audio Multicast RTCP** ” Ce port doit être le „Port audio Multicast“ plus 1.
“**Multicast TTL**” Time to Live (TTL).

Vous pouvez créer une redirection de port dans un router, en plus tous les ports peuvent toujours être retransmis. Ceci est nécessaire pour une communication réussie.



Configuration

- Système
- Sécurité
- Réseau
- LAN sans fil
- DDNS
- Liste d'accès
- Audio et vidéo
- Détection de mouvement
- Application
- Enregistrement
- Log de système
- Voir paramètres
- Maintenance

Version: 0101a

Home

Type de réseau

◉ LAN	
○ Obtenir adresse IP automatiquement	
◉ Utiliser adresse IP fixe	
Adresse IP	192.168.0.26
Masquage de sous-réseau	255.255.255.0
Routeur standard	192.168.0.1
DNS primaire	192.168.0.1
DNS secondaire	
Serveur WINS primaire	
Serveur WINS secondaire	
☑ Activer présentation UPnP	
☐ Activer transmission par port UPnP	
○ PPPoE	
Nom d'utilisateur	
Mot de passe	
Confirmer mot de passe	

Sauvegarder

HTTP

Authentification:	basic
Port HTTP	10060
Port HTTP secondaire	10061
Nom d'accès pour stream1	video.mjpg
Nom d'accès pour stream2	video2.mjpg

Audio bidirectionnel

Port audio bidirectionnel	5060

FTP

Port FTP	21

Streaming RTSP

Authentification:	disable
Nom d'accès pour stream1	live.sdp
Nom d'accès pour stream2	live2.sdp
Port RTSP	10062
Port RTP pour vidéo	10064
Port RTCP pour vidéo	10065
Port RTP pour audio	10066
Port RTCP pour audio	10067
Réglages Multicast pour stream 1	
☐ Toujours multicast	
Adresse de groupe Multicast	239.128.1.99
Port vidéo Multicast	5560
Port vidéo Multicast RTCP	5561
Port audio Multicast	5562
Port audio Multicast RTCP	5563
Multicast TTL [1~255]	15
Réglages Multicast pour stream 2	
☐ Toujours multicast	
Adresse de groupe Multicast	239.128.1.100
Port vidéo Multicast	5564
Port vidéo Multicast RTCP	5565
Port audio Multicast	5566
Port audio Multicast RTCP	5567
Multicast TTL [1~255]	15

Sauvegarder

« url » *http://“Network Camera“/setup/network.html*
« Network Camera » est le nom de domaine ou l’adresse IP par défaut de la caméra réseau .

« WLAN Configuration » (Wireless LAN)

« **SSID** » (Service Set Identifier) est le nom identifiant le réseau sans fil. Le point d'accès et la caméra réseau WLAN doivent utiliser le même nom SSID. La valeur par défaut est « default ». ATTENTION : la longueur maximale est de 32 caractères et les caractères : „ , ", <, > ainsi que les caractères d'espacement ne sont pas autorisés.

« **Mode sans fil** » Sélectionnez l'une des possibilités ci-dessous.

« **Infrastructure** » La caméra réseau est reliée au réseau par le biais d'un point d'accès.

« **Ad-Hoc »** Dans ce mode, une communication directe de la caméra réseau avec les autres adaptateurs réseau (carte réseau) est possible. Un environnement « Peer-to-Peer » est créé.

« **Canal** » En mode Infrastructure, le canal utilisé est sélectionné automatiquement par la caméra. En mode Ad-Hoc, le canal doit être configuré manuellement en fonction de l'autre adaptateur réseau.

« **Taux TX** » Réglez, à ce niveau, le débit réseau sur la valeur maximale. Par défaut, la sélection du débit est automatique (« auto »), en quoi la caméra essaie toujours d'obtenir le débit maximum disponible dans l'environnement.

« **Preamble** » Chacun des paquets est toujours précédé d'un préambule. Ce préambule permet de synchroniser la cadence du récepteur et de l'émetteur. Dans le cadre du « short preamble », la longueur de synchronisation est plus courte et donc moins sûre.

« **Sécurité** » Sélection de la méthode de chiffrement
« **Aucun** » Aucun chiffrement n'a été sélectionné.
« **WEP** » (Wired Equivalent Privacy) Une codage de 64 ou 128 bits est utilisée pour le chiffrement (HEX ou ASCII). La clé des deux appareils doit être la même pour que ceux-ci puissent communiquer.
« **WPA-PSK/WPA2-PSK** » (Wi-fi Protected Access - Pre Shared Keys) Cette méthode fait appel à des clés dynamiques.
La sélection des protocoles de chiffrement TKIP (Temporal Key Integrity Protocol) ou AES (Advanced Encrytion Standard) est possible.
Une « Pre-Shared-Key » doit être affectée en tant que clé.

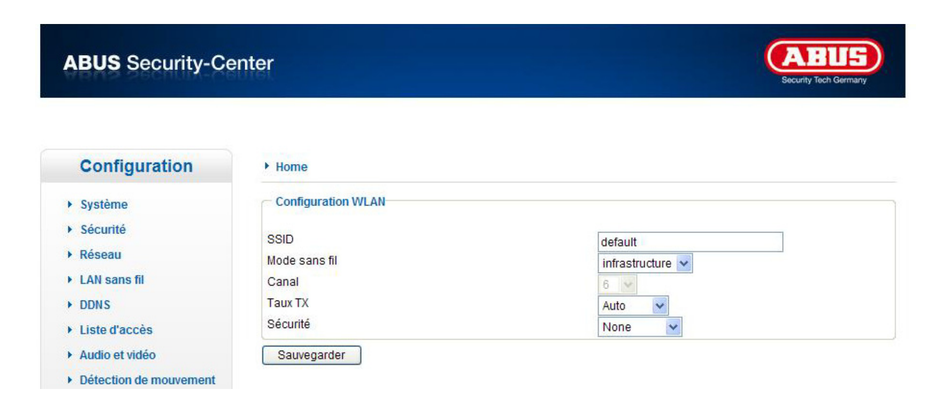
« **Auth mode** » mode d'authentification : sélectionnez l'une des méthodes suivantes.
« **Shared** » Ce mode permet uniquement la communication avec des appareils ayant la même clé WEP.
« **Open** » La clé est communiquée dans tout le réseau.

« **Key length** » Sélectionnez à ce niveau une longueur de clé de 64 ou de 128 bits.
« **Key format** » Format de clé
« **HEX** » Format hexadécimal
« **ASCII** » Format ASCII

« **Network key** » En présence de formats de clés différents, le système s'attend à des clés de longueur différente.
64 bits : 10 positions Hex ou 5 caractères
128 bits : 26 positions Hex ou 13 caractères
ATTENTION : si vous voulez utiliser les caractères 22 ("), 3C (<) ou 3E (>) pour la clé, l'utilisation du format ASCII n'est pas possible.

« **Pre-Shared-Key** » La saisie de cette clé a lieu en format ASCII avec une longueur de 8 à 63 caractères.

Un mauvais réglage peut interdire l'accès à la caméra. Si le système n'est plus accessible, lisez s.v.p les indices de reconstruction du réglage du système « regarder Annexe »



« url » *http://“Network Camera“/setup/wireless.html*
« Network Camera » est le nom de domaine ou l’adresse IP par défaut de la caméra réseau .

Ecran « DDNS

„**Activer DDNS**“ Cette option permet d'activer la fonction DDNS.
„**Fournisseur d’accès Internet**“ Cette liste présente 4 hôtes fournissant des services DDNS. Etablissez une connexion à la page du fournisseur de services pour être sûr que le service soit disponible.
„**Nom hôte** “ Ce champ doit être complété pour permettre l’utilisation du service DDNS. Entrez le nom d'hôte enregistré sur le serveur DDNS.
„**Nom d’utilisateur/Email**“ Le nom d’utilisateur et son adresse de messagerie doivent être indiqués dans ce champ pour permettre d'établir une connexion au serveur DDNS ou pour informer les utilisateurs de la nouvelle adresse IP. Remarque : si vous entrez le nom d’utilisateur dans ce champ, vous devez entrer le mot de passe dans le champ suivant.
„**Mot de passe**“ Entrez le mot de passe ou la touche pour utiliser le service DDNS.



« url » *http://“Network Camera“/setup/ddns.html*
« Network Camera » est le nom de domaine ou l’adresse IP par défaut de la caméra réseau .

Liste d'accès

« **Liste autorisée** » Cette zone permet d'entrer la page des IP acceptées et de l'ajouter à la liste d'accès. Toutes les IP sont acceptées par défaut. Supprimez, le cas échéant, l'intégralité de cette page.

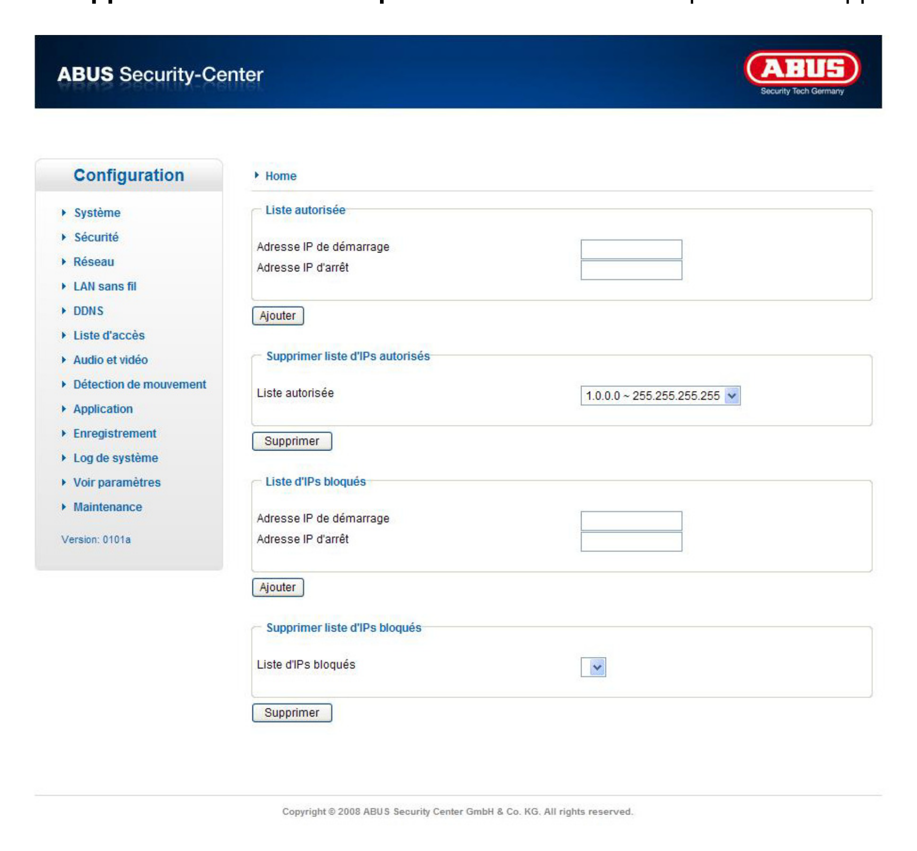
« **Adresse IP de démarrage** » Entrez dans ce champ la première adresse de la page souhaitée.

« **Adresse IP d'arrêt** » Entrez dans ce champ la dernière adresse de la page souhaitée.

« **Supprimer liste d'IPs autorisés** » Cette zone de liste permet de supprimer les pages souhaitées de la liste d'accès.

« **Liste d'IPs bloqués** » Ce champ permet de définir les pages IP à bloquer.

« **Supprimer liste d'IPs bloqués** » Cette zone de liste permet de supprimer des pages IP bloquées.

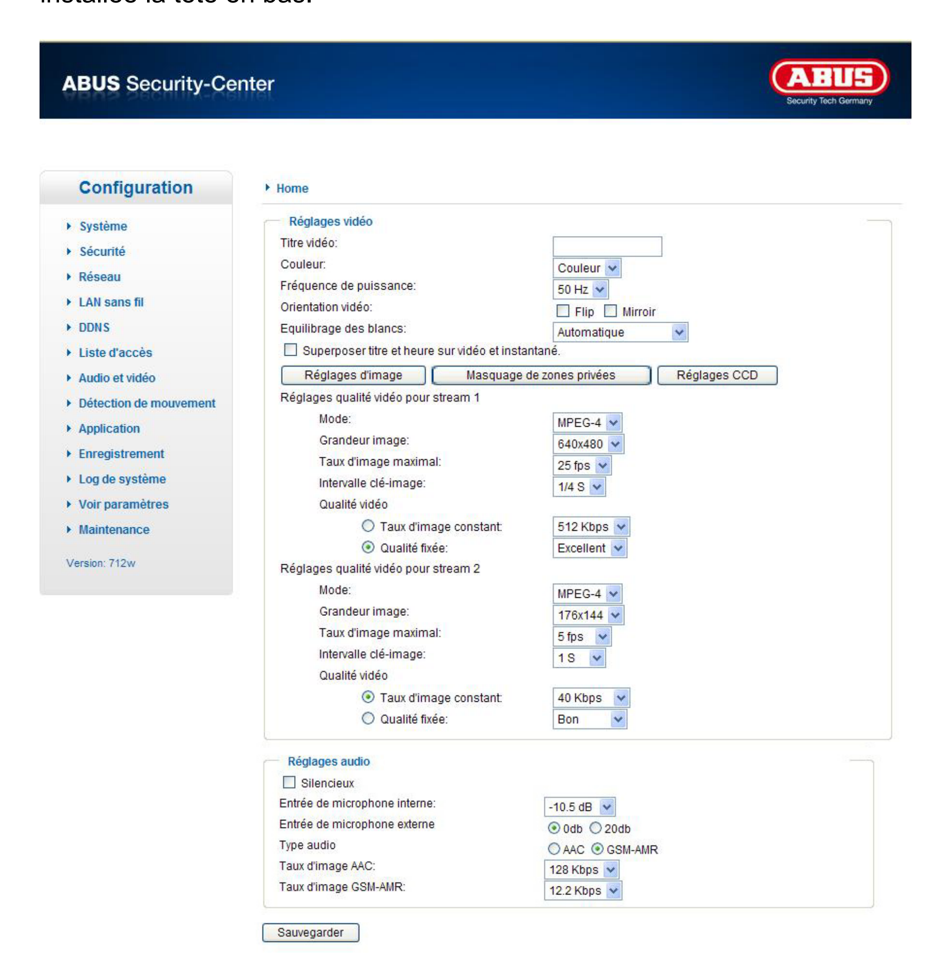


« url » *http://"Network Camera"/setup/accesslist.html*
« Network Camera » est le nom de domaine ou l'adresse IP par défaut de la caméra réseau .

Vidéo et audio

Ecran « Video »

„**Titre vidéo**“ Le texte apparaît dans la barre noire au-dessus de la fenêtre vidéo accompagné des informations de date enregistrées. Ces informations de date (date et heure) sont fournies par la caméra réseau et peuvent être retenues par le biais d'une horloge temps réel intégrée.
„**Couleur**“ Permet de choisir entre un affichage couleur ou noir et blanc.
Size Cinq options sont disponibles pour les trois tailles vidéo. “176x144”, “320x240” et “640x480”.
„**Fréquence de puissance**“ Lumière fluorescente pulsée à la fréquence secteur. Réglez la fréquence de manière à éliminer ces pulsations dans l'image.
„**Compression mode**“ Compression JPEG ou MPEG-4 disponible.
Trois paramètres en relation étroite sont disponibles pour la définition de la performance vidéo. „**Taux d'image maximal**“ Permet de limiter la fréquence d'images, qui combine au „**Qualité vidéo**“ permet d'améliorer l'utilisation de la bande passante et la qualité vidéo. Pour définir l'utilisation de la bande passante indépendamment de la qualité vidéo, il convient d'activer „**Taux d'image constant**“ et de sélectionner la bande passante souhaitée. L'envoi de la fréquence d'images maximale sur une bande passante limitée risque d'affecter la qualité vidéo lors de mouvements rapides sur les images. C'est la raison pour laquelle, afin de garantir une qualité vidéo (taux de quantification) indépendamment du réseau, la bande passante occupée est plus large pour permettre la gestion de la fréquence d'images maximale requise lors de l'envoi d'images de mouvements aux changements importants.
„**Flip**“ ermet la rotation verticale de la vidéo.
„**Mirroir**“ et la rotation horizontale de la vidéo. Sélectionnez ces options si la caméra réseau a été installée la tête en bas.



« Image settings »

Cliquez sur le bouton « **Réglages d'image**», pour faire apparaître la boîte de dialogue permettant de définir la luminosité, le contraste, la saturation et la teinte (Luminosité, Contraste, Saturation et Qualité) de l'image vidéo. Chaque champ dispose de 11 niveaux de -5 à +5. Un clic sur « **Préface**», permet de visualiser la configuration modifiée de l'image. Pour appliquer les paramètres d'image définis, cliquez sur « **Sauvegarder**». Un clic sur « **Restaurer**» permet d'ignorer les modifications apportées.
« Equilibrage des blancs» indiquez ici le nombre pour une température de couleur idéal



Masquage de zones privées

Grâce à cette fonction des sections peuvent être éteintes dans l'image vidéo. Au plus 5 grandes sections souhaitées peuvent être marquées.

Activez d'abord cette fonction en cochant l'option „Activer masquage de zones privées.

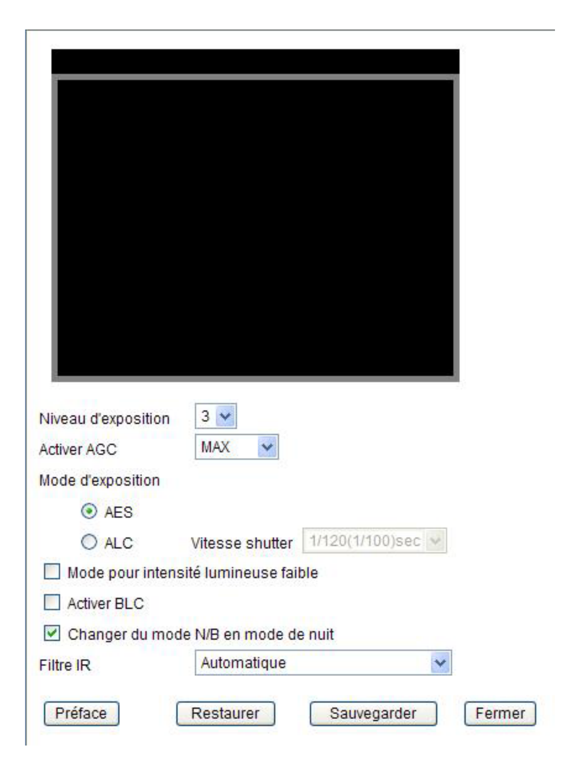
Grâce au bouton „Nouveau“ un nouvelle fenêtre sera montrée, la grandeur peut également être adaptée. Appuyez sur „Sauvegarder“ pour reprendre les réglages.



 Attention!
Cette fonction ne doit pas être activée, si des caméras pivotantes sont branchées.
⚠ Attention
Cette fonction ne peut qu'être configurée, si MS Internet Explorer est utilisé comme navigateur (mode ActiveX).

<URL> http://<Videoserver>/setup/privacy.html
<Videoserver> est l'adresse IP ou nom d'hôte du serveur web.

Configuration CCD



„L'étape d'exposition « mettez manuellement l'aperture d'IRIS d'objectif auto
„AGC“ Renforcement automatique: Normal ou Maximal
« AES » Auto Electronic Shutter
« ALC » Automatic Light Control, fixed shutter speed
« Mode » pour intensizé lumineuse faible » extends shutter time in low lux mode
„BLC“ Contre lumière: la reconnaissance des objets devant des sources lumineuses
„Options de commutation B/N en mode Nuit: Images blanche/noire pendant la nuit
„IR cut filter“ Options pour les phares IR:

- Auto: Commutation automatique à 2 Lux
- Agenda: Commutation par plan horaire
- Entrée digital: si l'entre est fermé, le mode de nuit est activé
- Mode Jour: activation manuelle de mode jour
- Mode Nuit: activation manuelle de mode nuit

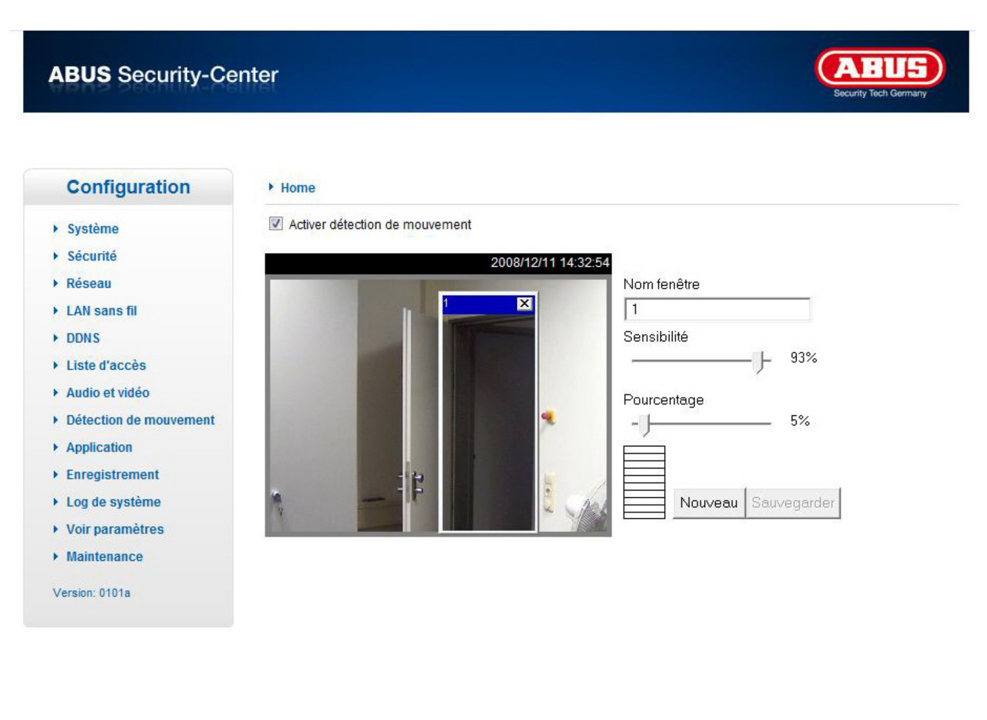
Configuration audio

« **Audio settings** » Sélectionnez ici le type audio et le bit rate souhaité.
« **AAC** » (Advanced Audio Coding) Codec spécial de compression audio dans le cadre de MPEG4.
« **GSM-AMR** » (Global System for Mobile Communications - Adaptive Multi Rate) Codec vocal du réseau GSM.

Ecran « Motion Detection »

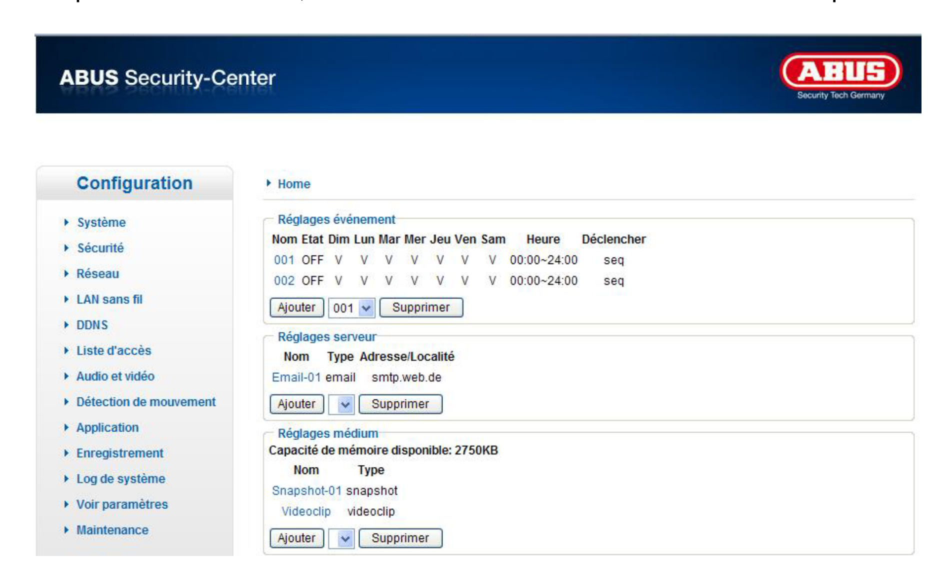
« **Activer masquage de zones privées** » Cochez cette case pour activer la détection de mouvement.
« **Nouveau** » Un clic sur ce bouton permet d'ajouter une fenêtre. Trois fenêtres peuvent au total être visualisées simultanément. Pour redimensionner la fenêtre ou déplacer la barre de titre, faites un clic gauche sur la bordure de la fenêtre et maintenez le bouton de la souris enfoncé, puis déplacez la bordure de la fenêtre jusqu'à obtenir la taille souhaitée. Un clic sur le 'x' dans le coin supérieur droit de la fenêtre permet de fermer cette dernière.
« **Sauvegarder**» Un clic sur ce bouton permet d'enregistrer les paramètres de la fenêtre correspondante. Une barre graphique augmente ou diminue en fonction de la variation de l'image. Une barre verte signifie que l'image varie au dessous du niveau de surveillance, tandis qu'une barre rouge signale une variation de l'image dépassant le niveau de surveillance. En présence d'une barre rouge, la fenêtre concernée apparaît également encadrée de rouge. La fenêtre surveillée disparaît au retour à la page d'accueil. Cependant, le cadre rouge est affiché dès qu'un mouvement est détecté.
« **Nom fenêtre** » le texte affiché dans ce champ apparaît en haut de la fenêtre.
« **Sensibilité** » sensibilité dans le cadre de modifications au niveau de l'image (ex. :sensibilité élevée : résolution lors de modifications minimes au niveau de l'image.
« **Pourcentage** » taille d'objet détectable (à pourcentage faible, le système détecte les objets de petite taille et à pourcentage élevé uniquement ceux de grande taille).

La figure ci-dessous présente l'écran affiché à l'issue d'un clic sur « **Sauvegarder**».



Application

La configuration d’application est composée de 3 sections: évènement, serveur et média. Pour configurer une action d’application la section „Médium“ doit d’abord être configurée, puis la section „Serveur“ et ensuite la section „Evènement“. Les sections sont décrites dans cet ordre.
Au plus 3 évènements, 5 entrées de serveur et 5 entrée de médias peuvent être créés.



<URL> http://<Videoserver>/setup/application.html
<Videoserver> est l’adresse IP ou le nom d’hôte du serveur web.

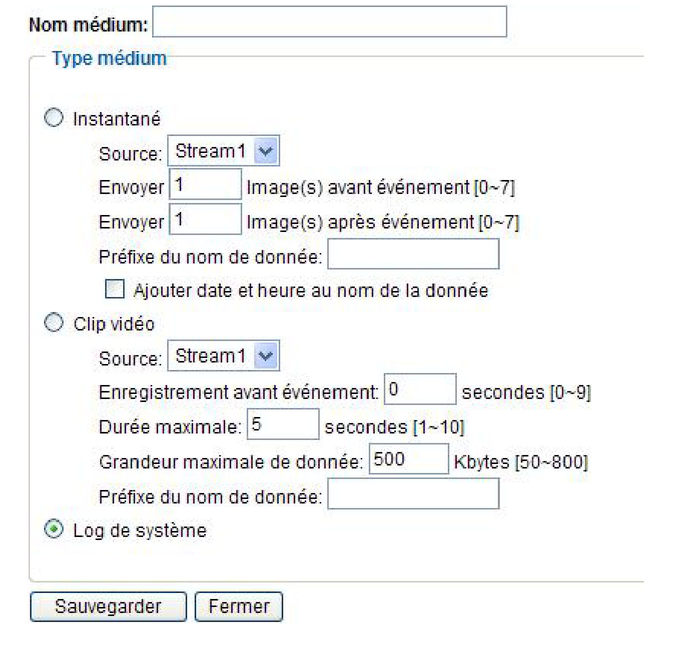
Médias

„**Nom des médias**“ Nom unique du médium. Il existe trois différents type de médias: instantané, clip vidéo ou log système.

Instantané

„**Source**“ L’enregistrement peut être effectué par stream vidéo 1 ou 2
„**Transmettre des images de pré-alarme**“ Nombre d’instantanés avant un événement.
„**Transmettre des images de post-alarme**“ Nombre d’instantanés après un événement.
„**Ajout au nom de donnée**“ Donnez ici une désignation qui précèdera le nom de la donnée en question pour l’instantané.
„**Attacher date et temps au nom de donnée**“ Avec cette option l’instantané enregistré est prévu de la date et le temps, afin de pouvoir distinguer les noms des instantanés de l’utilisation séquentielle et ceux de l’utilisation dirigée par des évènements. Exemple: video@20030102030405.jpg signifie que l’image JPEG du 2 janvier 2003 a été enregistrée à 3 heures, 4 minutes et 5 secondes. Si ce suffixe est supprimé, la donnée “video.jpg” sera actualisée sur le serveur FTP externe après le temps d’intervalle mentionné.

Clip vidéo

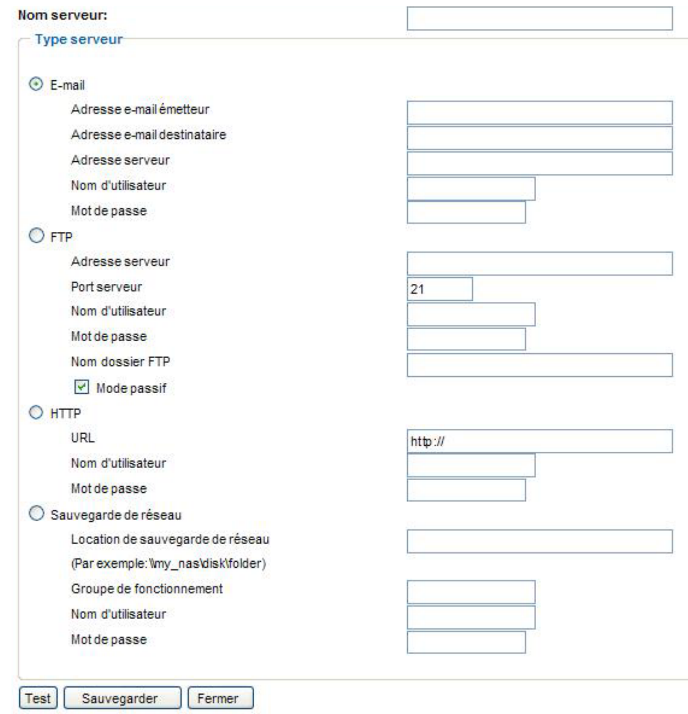


„**Source**“ L’enregistrement peut se faire par stream vidéo 1 ou 2.
„Enregistrement de pré-alarme“ Intervalle d’enregistrement de pré-alarme en secondes (max. 10 secondes)
„Durée maximale“ Durée maximale par donnée (max. 10 secondes)
„Grandeur maximale de donnée“ Grandeur maximale de la donnée en kByte (max. 800 kByte)
„**Ajouts au nom de donnée**“ Introduisez ici une désignation qui précèdera le nom de donnée de l’enregistrement vidéo.

Log système

Transmet le contenu actuel du log système.

Serveur



„**Nom serveur**“ Nom unique du serveur. Il existe 3 différents types de serveurs:
le serveur e-mail, le serveur FTP, le serveur http.

Serveur e-mail

„**Adresse e-mail expéditeur**“ L’adresse e-mail de l’expéditeur.
„**Adresse e-mail destinataire**“ L’adresse e-mail du destinataire.
„**Adresse de serveur**“ La désignation des domaines ou l’adresse IP du serveur e-mail.
„**Nom d’utilisateur**“ Nom d’utilisateur autorisé sur le serveur e-mail externe.
„**Mot de passe**“ Mot de passe autorisé sur le serveur e-mail externe.

Serveur FTP

„**Adresse serveur**“ La désignation des domaines ou l’adresse IP du serveur FTP externe.
„**Port serveur**“ Ce port peut être un autre port que le port 21 standard. L’utilisateur peut modifier ces paramètres de 1 à 65.535.
„**Nom d’utilisateur**“ Nom d’utilisateur autorisé sur le serveur FTP externe.
„**Mot de passe**“ Mot de passe autorisé sur le serveur FTP externe.
„**Changer le nom d’un dossier à distance**“ Dossier autorisé sur le serveur FTP externe. La chaîne de caractères doit correspondre à celle du serveur FTP externe. Quelques serveurs FTP ne peuvent pas accepter de barre oblique avant la désignation des chemins et sans reproduire le chemin virtuel. Les détails se trouvent dans le mode d’emploi du serveur FTP externe. Le privilège du dossier doit être ouvert avant le chargement.
„**Mode passif**“ Mode passif pour activer la transmission FTP. Cette technique est utilisée, si le client ne peut pas être atteint par le serveur (ex. client derrière router, barrière de sécurité).

Serveur http

„**URL**“ URL pour la mise à jour des médias.
„**Nom d’utilisateur**“ Nom d’utilisateur autorisé sur le serveur HTTP externe.
„**Mot de passe**“ Mot de passe autorisé sur le serveur e-mail externe.

Lecteur réseau

„**Mémoire du lecteur réseau**“ Le chemin d’un lecteur réseau en fonction de la mise à jour des médias.
„**Groupe de travail**“ Groupe de travail du lecteur réseau.
„**Nom d’utilisateur**“ Nom d’utilisateur autorisé du lecteur réseau.
„**Mot de passe**“ Mot de passe autorisé du lecteur réseau.

Après l’introduction des données du serveur, la connexion au serveur peut être testée par le bouton de commande „Test“. L’évènement sera affiché dans une fenêtre séparée.

Evènement

„**Nom d’évènement**“ Nom unique de l’évènement.
„**Evènement actif**“ Cocher pour activer l’évènement.
„**Priorité**“ Les évènements avec la plus grande priorité seront d’abord exécutés.
„**Temporisation de xx seconde(s) avant la détection du prochain évènement**“ Aucun nouvel évènement ne sera activé avant la terminaison de cette période, quoi qu’il est détecté par le capteur de mouvement ou l’entrée numérique.

Un évènement peut être activé selon 5 différentes méthodes:
„**Détection de mouvement**“ Choisissez la fenêtre, dans laquelle un mouvement doit être détecté.
„**Périodique**“ Un évènement est activé dans une intervalle définie (unité en minutes).
„**Redémarrage du système**“ Un évènement est activé par un redémarrage du système.

Horaires des évènements

“**Dim**” ~ “**Sam**” Sélectionne les jours de la semaine où l’évènement doit être effectué.
„**Toujours**“ Activation de l’événement à tout moment.
„**De**“ ~ „**à**“ L’évènement est temporairement limité.

Activer cet événement
Priorité: Normal
Détecter événement suivant après 10 seconde(s).
Déclencher
Détection de mouvement vidéo
Détecter mouvement dans fenêtre 1
Note: Veuillez configurer Détection de mouvement premier
Périodiquement
Déclencher chaque autre 1 minutes
Entrée digitale
Redémarrage système
Horaire événement
Dim Lun Mar Mer Jeu Ven Sam
Heure
Toujours
De 00:00 à 24:00 [hh:mm]
Action
Déclencher sortie numérique pour 1 secondes
Email-01
Médium attaché: -----None-----
Sauvegarder Fermer



Action

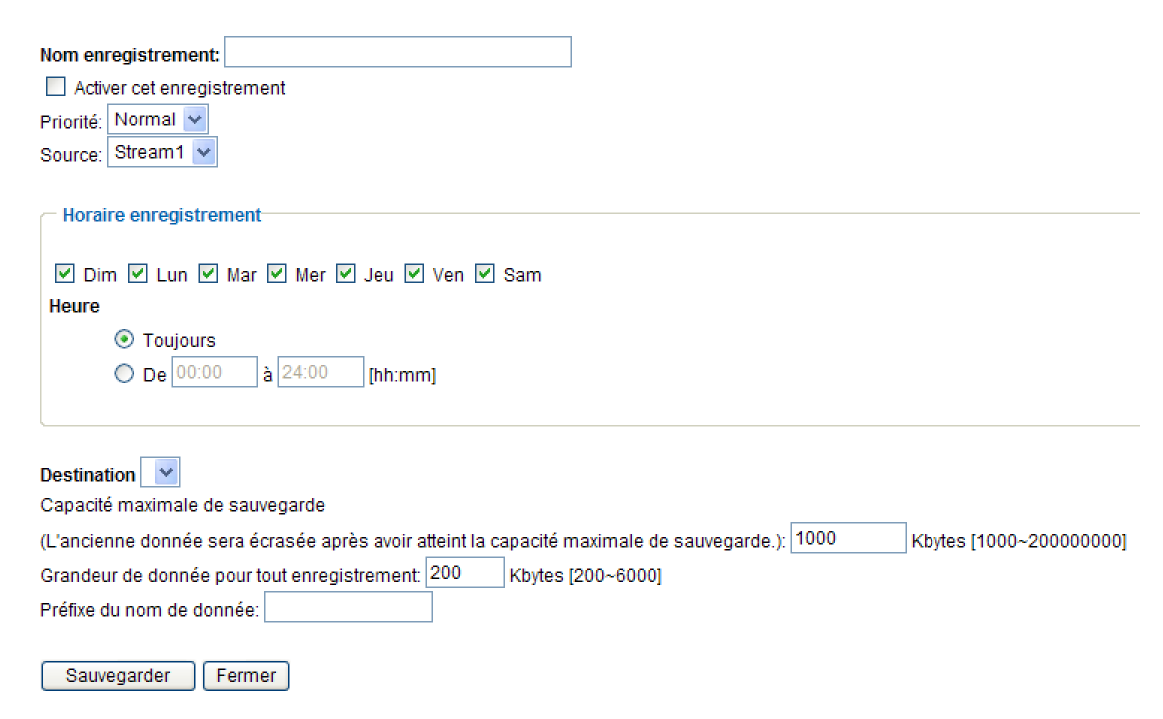
„**Serveur [Nom]**“ Le médium sélectionné est transmis au serveur en question (ex. un instantané est transmis à une adresse e-mail).

Enregistrement

Le camera supporte un enregistrement de données vidéo sur un lecteur réseau. Il est possible de configurer au plus 2 entrées d'enregistrement, mais d'abord un lecteur doit être configuré sous Application / Serveur / Lecteur réseau.

„**Entrée d'enregistrement**" Nom unique pour une entrée d'enregistrement.
„**Activer enregistrement**" Cocher afin d'activer une entrée d'enregistrement.
„**Priorité**" L'enregistrement avec la plus grande priorité sera d'abord effectué.
„**Source**" L'enregistrement peut se faire par stream vidéo 1 ou 2.
"**Dim**" ~ "**Sam**" Sélectionne le jour de la semaine où l'enregistrement doit être effectué.
„**Toujours**" Activation de l'enregistrement à tout moment.
„**De**" ~ „**à**" L'enregistrement est temporairement limité.

„**Destination**" Un des 2 lecteurs réseau.
„**Grandeur absolue de l'enregistrement circulaire**" Grandeur maximale de l'enregistrement circulaire en kByte.
„**Grandeur par donnée**" Après que la grandeur maximale est atteinte (Affichage en kByte), une nouvelle donnée sera lue. Quand la grandeur maximale de la mémoire circulaire est atteinte, la donnée la plus vieille sera effacée.
„**Ajouts au nom de donnée**" Désignation qui doit précéder le nom de donnée pour la distinction de ces données sur le lecteur réseau.



<URL> http://<Videoserver>/setup/recording.html
<Videoserver> est l'adresse IP ou le nom d'hôte du serveur vidéo

« Log de système »

Un clic sur ce lien de l'écran de configuration permet d'afficher le fichier journal système. Ce fichier fournit des informations utiles sur la configuration et la connexion à l'issue du démarrage du système. RFC 3164 est le standard du fichier journal. Vous pouvez également envoyer des données à un serveur de fichiers journaux. Activez à cet effet l'option „Remote Protokoll", et entrez l'adresse IP ainsi que le numéro de port du serveur.

« Voir paramètres »

Un clic sur ce lien de l'écran de configuration permet d'afficher tous les jeux de paramètres système. Le contenu de ce fichier correspond à celui du fichier CONFIG.INI.

Administration (Maintanance)

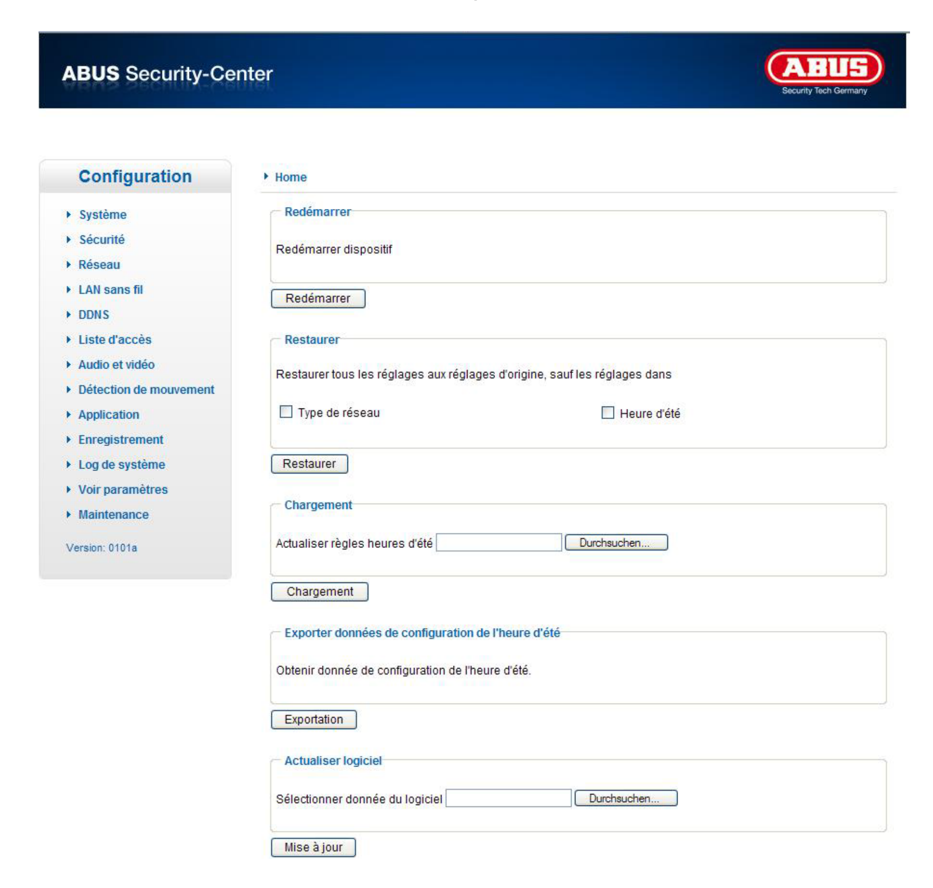
Redémarrage du système /Reboot
Un clic sur ce lien de l'écran de configuration permet de redémarrer le système.

« Restaurer »

Un clic sur ce lien de l'écran de configuration permet de rétablir l'intégralité de la configuration d'origine. Toutes les modifications apportées sont annulées et le système rétablit les paramètres à la sortie d'usine.
A l'issue d'un clic sur « Restaurer » et de la validation de l'opération, le système redémarre et exige le programme d'installation, afin d'installer et de configurer de nouveau le réseau.

Firmware Update / progiciels Actualiser logiciel

Ici aussi il y a la possibilité d'actualiser le progiciel.
Les progiciels actuels sont disponibles sur le site www.abus-sc.com .Choisissez le fichier Update et appuyez sur l'écran « Mise à jour ». La mise á jour prend un peut de temps. Après le redémarrage, la caméra sera fournie du nouveau progiciel.



Annexe

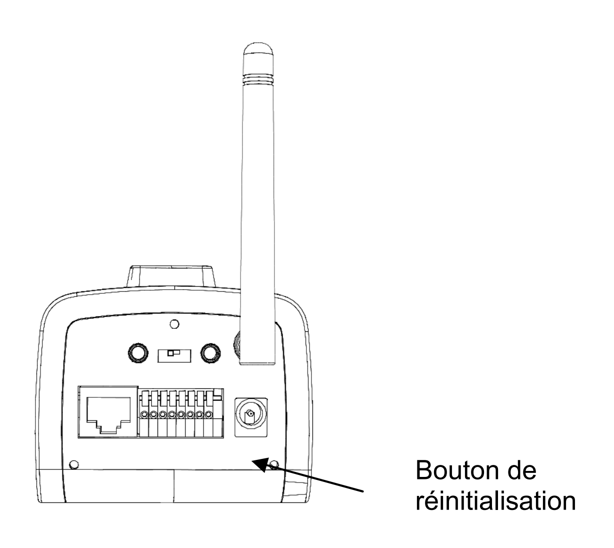
A. Troubleshooting

Status LED

Couleur du LED	Vert	Rouge
Mise en tension	activé	1/s (1 fois)
Procès Boot	désactivé	1/s
Configuration/recherche de réseau	activé	désactivé
Réseau ok	1/s	activé
Mise a jour du micro logiciel	1/s	0.1/s

Réinitialisation et rétablissement

Le Bouton de réinitialisation est situé sur la face arrière de la camera , une réinitialisation suffit au retour du système à l'état normal. Cependant, si des problèmes persistent à l’issue de la réinitialisation, rétablissez la configuration d’origine, puis installez et configurez de nouveau le système.



Le rétablissement de la configuration d’origine permet de supprimer les paramètres définis auparavant. Le système peut être réinitialisé ou rétabli.

REINITIALISATION :
Pressez le bouton de réinitialisation à l’aide d’un objet pointu.

RETABLISSEMENT :
1. Pressez sur le bouton de manière continue avec un objet pointu.
2. Attendez jusqu’à ce que toutes les LEDs clignotent rapidement.
3. Relâchez le bouton de réinitialisation, dès que le second autotest démarre.

B. Questions fréquemment posées (FAQ)

Q. Que faire lorsque vous avez oublié le mot de passe ?
R. Tout accès à la caméra réseau nécessite une authentification. Si vous êtes l'un des utilisateurs chargés de tâches gestion, adressez-vous à l'administrateur pour obtenir le mot de passe. Si vous êtes administrateur, vous ne disposez d'aucune possibilité de récupération du mot de passe « root ». La seule possibilité restante d'accès à la caméra réseau consiste à presser le bouton de réinitialisation permettant de rétablir la configuration d'origine en face arrière de l'appareil, puis de reconfigurer le système.

Q. Pourquoi le système n'affiche-t-il pas de vidéo sur la caméra réseau à l'issue de l'authentification ?
R. Ce problème peut avoir différentes causes :
1. Si vous venez juste d'installer la caméra réseau et que vous ne pouvez pas visualiser de vidéo, vérifiez la modulation vidéo au niveau de l'écran de configuration.
2. Réduisez le niveau de sécurité d'Internet Explorer pour permettre l'installation du plug-in.
3. Si le problème persiste, il se peut que les utilisateurs utilisent un niveau de sécurité plus élevé que celui autorisé par le système.

Q. A quoi sert le plug-in ?
R. Le plug-in mis à disposition par la caméra permet d'afficher des séquences vidéo dans Internet Explorer. Si le système n'autorise pas l'utilisation d'un plug-in, il convient de réduire le niveau de sécurité du navigateur Internet. Il est recommandé de s'adresser à l'administrateur réseau.

Q. Pourquoi les informations de date et d'heure enregistrées sont-elles différentes de l'heure système du PC ou de l'ordinateur portable ?
R. Les données de date et d'heure enregistrées sont axées sur l'heure système de la caméra réseau . Celle-ci est retenue par l'horloge temps réel interne et peut être synchronisée automatiquement avec un serveur horaire, si la caméra réseau est reliée à l'Internet et que la fonction correspondante a été activée. Les écarts de plusieurs heures sont liés aux fuseaux horaires.

Q. Pourquoi la mise à jour de l'image n'est-elle pas régulière ?
R. Dans un environnement modem, ceci est lié au fait que la bande passante de la liaison PPP est nettement plus faible que dans un environnement Ethernet. Si l'écart des données de date et d'heure enregistrées est instable, réduisez l'UART FIFO pour la réception et la transmission au niveau des propriétés Modem du Panneau de configuration. Dans Ethernet, ceci peut être lié à la durée nécessaire à la mise en mémoire de l'instantané, lorsque l'événement survient.

Q. Combien d'utilisateurs peuvent visualiser simultanément la vidéo ?
R. En principe, le nombre est limité sur 20 utilisateurs . Cependant, la qualité vidéo dépend de la bande passante réseau.

Q. Quelle est la fréquence d'images vidéo de la caméra réseau ?
R. Le codec MPEG4 est à même de traiter en interne 30 images par seconde. Cependant, la performance globale dépend de divers facteurs :
1. du débit réseau,
2. de la bande passante partagée,
3. du nombre d'utilisateurs,
4. des objets visibles « complexes » qui entraînent des fichiers d'images plus volumineux,
5. de la configuration PC chargée de l'affichage des images.
En général, dans un réseau local courant, le débit peut dépasser 200 Ko par seconde et près de 10 à 20 images par seconde.

Q. Comment l'accès aux séquences vidéo de la caméra réseau peut-il être sécurisé au maximum ?
R. La caméra réseau a été développée à des fins de surveillance et elle est équipée d'un grand nombre d'interfaces flexibles. L'authentification des utilisateurs et la confirmation spéciale lors de l'installation peuvent empêcher un accès frauduleux à la caméra réseau . Vous pouvez également changer le numéro du port HTTP et sélectionner un numéro non public. Vérifiez le journal système à la recherche d'activités anormales et trouvez-en la cause.

Q. Dans quelle mesure la caméra réseau est-elle capable de contrôler rapidement l'état des entrées numériques ?
R. La caméra réseau vérifie l'état de l'entrée en moins d'une demi-seconde. Cependant, afin d'éviter les conditions d'un contrôle réitéré et pour assurer le fonctionnement correct des périphériques reliés aux sorties numériques, la caméra réseau temporise de 3 seconde à l'issue de chaque adaptation de la condition. Les utilisateurs peuvent adapter cela en fonction des applications spécifiques. Pendant ce délai, le système ignore les autres conditions.

Q. Pourquoi l'accès à la caméra réseau est-il impossible lorsque certaines options de l'application ont été définies ?
R. Lors du déclenchement de la caméra réseau par des événements, les enregistrements instantanés nécessitent plus de temps, car ils doivent être mis en mémoire. Si des événements surviennent souvent, le système est occupé à mettre les images en mémoire. Lorsque l'événement survient fréquemment, l'utilisation du mode séquentiel ou d'un programme d'enregistrement externe est recommandé pour enregistrer les images vidéo. Si vous voulez obtenir les images par FTP, le paramètre peut être moins élevé, car la réponse FTP est plus rapide que la réponse Web. Si la charge de travail du système est trop importante pour la configuration, utilisez la configuration d'origine et pressez le bouton de réinitialisation pour l'enregistrement du système.

Q. La caméra a été configurée correctement. Cependant, l'accès à la caméra via le protocole http ou RTSP est refusé.
R. Assurez-vous que les ports correspondants (par défaut : port 80 ou 554) soient activés dans les routeurs ou firewall éventuellement utilisés. Testez également le protocole réseau « Ping » (invite Windows : ping <adresse IP>).

Q. La caméra réseau est reliée au réseau par le biais d'un routeur. Cependant, l'accès à la caméra est refusé.
R. Si vous voulez relier la caméra au réseau par le biais d'un routeur (passerelle), vous devez affecter l'IP de la passerelle (routeur par défaut). Ceci n'est possible qu'à l'issue du raccordement direct de la caméra par un câble à paire torsadée, puis la configuration de la caméra.

Q. La caméra réseau est en aval d'un routeur avec une adresse IP. Comment accéder à la caméra concernée via Internet ?
R. Le routeur reçoit, lors d'une numérotation modem (par ex. DSL), une IP publique directement accessible à tous. Le transmission , par ex. d'une requête http issue de l'Internet, est envoyé en premier à l'IP publique. Le routeur doit être configuré de manière à ce que cette requête soit communiquée à l'IP locale. Consultez à cet effet dans la documentation fournie avec votre routeur les termes ci-dessous : NAT (Network Adresse Translation, IP forwarding, serveur IP).

C. URL-Commands

Style convention

In URL syntax and in descriptions of CGI parameters, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string also the angle brackets shall be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example, also below.

URL syntax' are written with the "**Syntax:**" word written in bold face followed by a box with the referred syntax as seen below. The name of the server is written as <servername>. This is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Special note will be marked as RED words to take care.

Syntax:

http://<*servername*>/cgi-bin/viewer/video.jpg

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data returned as HTTP formatted, i.e., starting with the string HTTP is line separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

HTTP/1.0 <HTTP code> <HTTP text>\r\n

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

http://mywebserver/cgi-bin/viewer/video.jpg

General CGI URL syntax and parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, the internal parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in function related directories under the cgi-bin directory. The file extension of the CGI is required.

Syntax:

http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*> [?<parameter>=<value>[&<parameter>=<value>...]]

Example: Setting digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

Security level

SECURITY	SUB-DIRECTORY	DESCRIPTION

LEVEL		
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera 2. Can control dido, ptz of camera
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator's access right can modify most of camera's parameters except some privilege and network options
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator's access right can fully control the camera's operation.
7	N/A	Internal parameters. Unable to be changed by any external interface.

Get server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/viewer/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/operator/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]
[&<parameter>…]
```

where the *<parameter>* should be *<group>*[_*<name>*] or *<group>*[.*<name>*] If you do not specify the any parameters, all the parameters on the server will be returned. If you specify only *<group>*, the parameters of related group will be returned.

When query parameter values, the current parameter value are returned.

Successful control request returns paramter pairs as follows.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
```

```
\r\n
<parameter pair>
```

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.

Example: request IP address and it's response

```
Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Set server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://<servername>/cgi-bin/viewer/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<servername>/cgi-bin/operator/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<servername>/cgi-bin/admin/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign *<value>* to the parameter *<group>*_*<name>*

update	<boolean>	set to 1 to actually update all fields (no need to use update parameter in each group)
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page. (note: The return page can be a general HTML file(.htm, .html) or a Vivotek server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]
Only the parameters that you set and readable will be returned.

Example: Set the IP address of server to 192.168.0.123

Request:
http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

Available parameters on the server
Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text string shorter than 'n' characters
password[<n>]	The same as string but display '*' instead

integer	Any number between $(-2^{31} - 1)$ and $(2^{31} - 1)$
positive integer	Any number between 0 and $(2^{32} - 1)$
<m> ~ <n>	Any number between 'm' and 'n'
domain name[<n>]	A string limited to contain a domain name shorter than 'n' characters (eg. www.ibm.com)
email address [<n>]	A string limited to contain a email address shorter than 'n' characters (eg. joe@www.ibm.com)
ip address	A string limited to contain an ip address (eg. 192.168.1.1)
mac address	A string limited to contain mac address without hyphen or colon connected
boolean	A boolean value 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string
everything inside <>	As description

NOTE: The camera should prevent to restart when parameter changed.

Group: **system**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	host name of server
ledoff	<boolean>	6/6	turn on(0) or turn off(1) all led indicators
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to 'keep' keeping date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current time of system. Set to 'keep' keeping time unchanged. Set to 'auto' to use NTP to synchronize time.
ntp	<domain name>, <ip address>,	6/6	NTP server

	<blank>		
timezoneindex	-489 ~ 529	6/6	Indicate timezone and area -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -160: GMT-04:00 Atlantic Time, Canada, Caracas ,La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time:Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait,

			Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval.

restore	0, <positive integer>	7/6	Restore the system parameters to default value. Restart the server after <value> seconds.
reset	0, <positive integer>	7/6	Restart the server after <value> seconds.
restoreexceptnet	0, <positive integer>	7/6	Restore the system parameters to default value except (ipaddress, subnet, router, dns1, dns2, ddns settings). Restart the server after <value> seconds.

SubGroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	0/7	model name of server
serialnumber	<mac address>	0/7	12 characters mac address without hyphen connected
firmwareversion	string[40]	0/7	The version of firmware, including model, company, and version number in the format <MODEL-BRAND-VERSION>
language_default	string[16]	0/7	Default webpage language.
language_count	<integer>	0/7	number of webpage language available on the server
language_i<0~(count-1)>	string[16]	0/7	Available language lists

Group: **status**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~ndi-1)>	<boolean>	1/1	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	6/7	current RTSP connection numbers
onlinenum_httppush	integer	6/7	current HTTP push server connection numbers

Group: **di_i<0~(ndi-1)>**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	1/1	indicate whether open circuit or closed circuit represents inactive status

Group: **do_i<0~(ndo-1)>**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	indicate whether open circuit or closed circuit represents inactive status

Group: security

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user_i0_name	string[64]	6/7	User's name of root
user_i<1~20>_name	string[64]	6/7	User's name
user_i0_pass	string [64]	6/6	Root's password
user_i<1~20>_pass	string [64]	7/6	User's password
user_i0_privilege	admin	6/7	Root's privilege
user_i<1~20>_ privilege	viewer, operator, admin	6/6	User's privilege.

Group: **network**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	6/6	Network connection type
resetip	<boolean>	6/6	1 => get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot

			0 => use preset ipaddress, subnet, rounter, dns1, and dns2
ipaddress	<ip address>	6/6	IP address of server
subnet	<ip address>	6/6	subnet mask
router	<ip address>	6/6	default gateway
dns1	<ip address>	6/6	primary DNS server
dns2	<ip address>	6/6	secondary DNS server
wins1	<ip address>	6/6	primary WINS server
wins2	<ip address>	6/6	secondary WINS server

Subgroup of **network**: **ftp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	6/6	local ftp server port

Subgroup of **network**: **http**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	6/6	HTTP port
alternateport	1025~65535	6/6	Alternative HTTP port
authmode	basic, digest	1/6	HTTP authentication mode
s0_accessname	string[32]	1/6	Http server push access name for stream 1
s1_accessname	string[32]	1/6	Http server push access name for stream 2

Subgroup of **network**: **rtsp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	6/6	RTSP port
authmode	disable,	1/6	RTSP authentication mode

	basic, digest		
s0_accessname	string[32]	1/6	RTSP access name for stream1
s1_accessname	string[32]	1/6	RTSP access name for stream2

Subgroup of **rtsp_s<0~(n-1)>**: **multicast,** n is stream count

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast
ipaddress	<ip address>	4/4	Multicast IP address
videoport	1025 ~ 65535	4/4	Multicast video port
audioport	1025 ~ 65535	4/4	Multicast audio port
ttl	1 ~ 255	4/4	Mutlicast time to live value

Subgroup of **network**: **rtp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	6/6	video channel port for RTP
audioport	1025 ~ 65535	6/6	audio channel port for RTP

Subgroup of **network**: **pppoe**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user	string[128]	6/6	PPPoE account user name
pass	password[64]	6/6	PPPoE account password

Group: ipfilter

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Allowed starting IP address for RTSP connection
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Allowed ending IP address for RTSP connection

deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Denied starting IP address for RTSP connection
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Denied ending IP address for RTSP connection

Group: **videoin**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
freq	50, 60	4/4	frequency
whitebalance	auto, indoor, fluorescent, outdoor	4/4	auto, auto white balance indoor, 3200K fluorescent, 5500K outdoor, > 5500K

Group: **videoin_c<0~(n-1)>** for n channel products, m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
color	0, 1	4/4	0 =>monochrome 1 => color
flip	<boolean>	4/4	flip the image
mirror	<boolean>	4/4	mirror the image
ptzstatus	<integer>	1/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support camera control function 0(not support), 1(support) Bit 1 => **Build-in** or **external** camera. 0(external), 1(build-in) Bit 2 => Support **pan** operation. 0(not support), 1(support) Bit 3 => Support **tilt** operation. 0(not support), 1(support) Bit 4 => Support **zoom** operation. 0(not support), 1(support) Bit 5 => Support **focus** operation. 0(not support), 1(support)
text	string[16]	4/4	enclosed caption
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video
maxexposure	1~120	4/4	Maximum exposure time

s<0~(m-1)>_codectype	mpeg4, mjpeg	4/4	video codec type
s<0~(m-1)>_keyinterval	1, 3, 5, 10, 30, 60, 90, 120	4/4	Key frame interval
s<0~(m-1)>_resolution	176x144, 320x240, 640x480,,	4/4	Video resolution in pixel
s<0~(m-1)>_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_quant	1, 2, 3, 4, 5	4/4	quality of video when choosing vbr in “ratecontrolmode”. 1 is worst quality and 5 is the best quality.
s<0~(m-1)>_bitrate	20000, 30000, 40000, 50000, 64000, 128000, 256000, 384000, 512000, 768000, 1000000, 1200000, 1500000, 2000000, 3000000, 4000000	4/4	set bit rate in bps when choose cbr in “ratecontrolmode”
s<0~(m-1)>_maxframe	1, 2, 3, 5, 10, 15, 20, 25, 30 (only for NTSC or 60Hz)	4/4	set maximum frame rate in fps
s<0~(m-1)>_forcei	1	7/6	Force I frame

Group: **audioin_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
source	micin, linein	4/4	micin => use external microphone input linein => use line input, i.e. internal

			microphone
mute	0, 1	4/4	Enable audio mute
gain	0~31	4/4	Gain of input
boostmic	0, 1	4/4	Enable microphone boost
s<0~(m-1)>_codectype	aac4, gamr	4/4	set audio codec type for input
s<0~(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	4/4	set AAC4 bitrate in bps
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	set AMR bitrate in bps

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
hue	-5 ~ 5	4/4	Adjust hue of image according to mode settings.

Group: **motion_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION

enable	<boolean>	4/4	enable motion detection
win_i<0~2>_enable	<boolean>	4/4	enable motion window 1~3
win_i <0~2>_name	string[14]	4/4	name of motion window 1~3
win_i <0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
win_i <0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
win_i <0~2>_width	0 ~ 320	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.

Group: **ddns**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the dynamic dns.
provider	Safe100, DyndnsDynamic, DyndnsCustom, TZO, DHS, DynInterfree, PeanutHull, CustomSafe100	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) TZO => tzo.com DHS => dhs.org DynInterfree =>dyn-interfree.it PeanutHull => peanut hull CustomSafe100 => Custom server using safe100 method
<provider>_hostname	string[128]	6/6	Your dynamic hostname.
<provider>_usernameemail	string[64]	6/6	Your user or email to login ddns service provider
<provider>_passwordkey	string[64]	6/6	Your password or key to login ddns service provider
<provider>_servername	string[128]	6/6	The server name for safe100. (This field only exists for provider is customsafe100)

Group: upnppresentation

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP presentation service.

Group: upnpportforwarding

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP port forwarding service.
upnpnatstatus	0~3	6/7	The status of UpnP port forwarding, used internally. 0 is OK, 1 is FAIL, 2 is no IGD router, 3 is no need to do port forwarding

Group: **syslog**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	6/6	enable remote log
serverip	<IP address>	6/6	Log server IP address
serverport	514, 1025~65535	6/6	Server port used for log
level	0~7	6/6	The levels to distinguish the importance of information. 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable the privacy mask

win_i<0~4>_enable	<boolean>	4/4	Enable the privacy mask window
win_i<0~4>_name	string[14]	4/4	The name of privacy mask window
win_i<0~4>_left	0 ~ 320/352	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240/288	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320/352	4/4	Width of privacy mask window
win_i<0~4>_height	0 ~ 240/288	4/4	Height of privacy mask window

Group: capability

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_http_version	0200a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	The server bootup time
nir	0, <positive integer>	0/7	number of IR interface
ndi	0, <positive integer>	0/7	number of digital input
ndo	0, <positive integer>	0/7	number of digital output
naudioin	0, <positive integer>	0/7	number of audio input
naudioout	0, <positive integer>	0/7	number of audio output
nvideoin	<positive integer>	0/7	number of video input
nmediastream	<positive integer>	0/7	number of media stream per channel
nvideosetting	<positive integer>	0/7	number of video settings per channel
naudiosetting	<positive integer>	0/7	number of audio settings per channel
nuart	0, <positive integer>	0/7	number of UART interface
ptzenabled	< boolean >	0/7	indicate whether to support PTZ control
protocol_https	< boolean >	0/7	indicate whether to support http over SSL

protocol_rtsp	< boolean >	0/7	indicate whether to support rtsp
protocol_sip	<boolean>	0/7	indicate whether to support sip
protocol_maxconnection	<positive integer>	0/7	The maximum allowed simultaneous connections
protocol_rtp_multicast_ scalable	<boolean>	0/7	indicate whether to support scalable multicast
protocol_rtp_multicast_ backchannel	<boolean>	0/7	indicate whether to support backchannel multicast
protocol_rtp_tcp	<boolean>	0/7	indicate whether to support rtp over tcp
protocol_rtp_http	<boolean>	0/7	indicate whether to support rtp over http
protocol_spush_mjpeg	<boolean>	0/7	indicate whether to support server push motion jpeg
protocol_snmp	<boolean>	0/7	indicate whether to support snmp
videoin_type	0, 1, 2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 =>
videoin_resolution	<a list of the available resolution separates by comma)	0/7	available resolutions list
videoin_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
videoout_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
audio_aec	<boolean>	0/7	indicate whether to support acoustic echo cancellation
audio_extmic	<boolean>	0/7	indicate whether to support external microphone input
audio_linein	<boolean>	0/7	indicate whether to support external line input
audio_lineout	<boolean>	0/7	indicate whether to support line output
audio_headphoneout	<boolean>	0/7	indicate whether to support headphone output

audioin_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
audioout_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
camctrl_httptunnel	<boolean>	0/7	Indicate whether to support the http tunnel for camera control
uart_httptunnel	<boolean>	0/7	Indicate whether to support the http tunnel for uart transfer
transmission_mode	Tx, Rx, Both	0/7	Indicate what kind of transmission mode the machine used. TX: server, Rx: receiver box, Both: DVR?.
network_wire	<boolean>	0/7	Indicate whether to support the Ethernet
network_wireless	<boolean>	0/7	Indicate whether to support the wireless
wireless_802dot11b	<boolean>	0/7	Indicate whether to support the wireless 802.11b+
wireless_802dot11g	<boolean>	0/7	Indicate whether to support the wireless 802.11g
wireless_encrypt_wep	<boolean>	0/7	Indicate whether to support the wireless WEP
wireless_encrypt_wpa	<boolean>	0/7	Indicate whether to support the wireless WPA
wireless_encrypt_wpa2	<boolean>	0/7	Indicate whether to support the wireless WPA2

Group: event_i<0~2>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
enable	0, 1	6/6	To enable or disable this event.
priority	0, 1, 2	6/6	Indicate the priority of this event. “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.

delay	1~999	6/6	Delay seconds before detect next event.
trigger	boot, di, motion, seq,	6/6	Indicate the trigger condition. “boot” indicates system boot. “di” indicates digital input. “motion” indicates video motion detection. “seq” indicates periodic condition.
di	<integer>	6/6	Indicate which di detected. This field is required when trigger condition is “di”. One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	6/6	Indicate which motion detection windows detected. This field is required when trigger condition is “md”. One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
inter	1~999	6/6	Interval of period snapshot in minute. This field is used when trigger condition is “seq”.
weekday	<interger>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates Sunday. For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Begin time of weekly schedule.
endtime	hh:mm	6/6	End time of weekly schedule. (00:00 ~ 24:00 means always.)
action_do_i<0~(ndo-1)>_enable	0, 1	6/6	To enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	6/6	The duration of digital output is triggered in seconds.

action_server_i<0~4>_enable	0, 1	6/6	To enable or disable this server action. The default value is 0.
action_server_i<0~4>_media	NULL, 0~4	6/6	The index of attached media.

Group: server_i<0~4>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
type	email, ftp, http, ns	6/6	Indicate the server type. “email” is email server. “ftp” is ftp server. “http” is http server. “ns” is network storage.
http_url	string[128]	6/6	The url of http server to upload.
http_username	string[64]	6/6	The username to login in the server.
http_passwd	string[64]	6/6	The password of the user.
ftp_address	string[128]	6/6	The ftp server address
ftp_username	string[64]	6/6	The username to login in the server.
ftp_passwd	string[64]	6/6	The password of the user.
ftp_port	0~65535	6/6	The port to connect the server.
ftp_location	string[128]	6/6	The location to upload or store the media.
ftp_passive	0, 1	6/6	To enable or disable the passive mode. 0 is to disable the passive mode. 1 is to enable the passive mode.
email_address	string[128]	6/6	The email server address
email_username	string[64]	6/6	The username to login in the server.
email_passwd	string[64]	6/6	The password of the user.
email_senderemail	string[128]	6/6	The email address of sender.
email_recipientemail	string[128]	6/6	The email address of recipient.
ns_location	string[128]	6/6	The location to upload or store the media.
ns_username	string[64]	6/6	The username to login in the server.

ns_passwd	string[64]	6/6	The password of the user.
ns_workgroup	string[64]	6/6	The workgroup for network storage.

Group: media_i<0~4>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
type	snapshot, systemlog videoclip	6/6	The media type to send to the server or store by the server.
snapshot_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
snapshot_prefix	string[16]	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	6/6	To add date and time suffix to filename or not. 1 means to add date and time suffix. 0 means not to add it.
snapshot_preevent	0 ~ 7	6/6	It indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	6/6	The number of post-event images.
videoclip_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
videoclip_prefix	string[16]	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	6/6	It indicates the time of pre-event recording in seconds.
videoclip_maxduration	1 ~ 10	6/6	The time of maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 1500	6/6	The maximum size of one video clip file in Kbytes.

Group: record_i<0~1>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry

enable	0, 1	6/6	To enable or disable this recoding.
priority	0, 1, 2	6/6	Indicate the priority of this recoding. “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
weekday	<interger>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates Sunday. For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Begin time of weekly schedule.
endtime	hh:mm	6/6	End time of weekly schedule. (00:00~24:00 means always.)
prefix	string[16]	6/6	Indicate the prefix of the filename.
cyclesize	<integer>	6/6	The maximum size for cycle recording in Kbytes.
maxfilesize	200~6000	6/6	The max size for one file in Kbytes

Drive the digital output

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/setdo.cgi?do1=<*state*>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<*return page*>]

Where state is 0, 1. “0” means inactive or normal state while “1” means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – inactive, normal state
		1 – active, triggered state
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

Example: Drive the digital output 1 to triggered state and redirect to an empty page

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

Query status of the digital input

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]

If no parameter is specified, all the status of digital input will be returned.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <*length*>\r\n
\r\n
[di0=<state>*]\r\n*
[di1=<state>*]\r\n*
[di2=<state>*]\r\n*
[di3=<state>*]\r\n*

where <*state*> can be 0 or 1.

Example: Query the status of digital input 1

Request:
http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:
HTTP/1.0 200 OK\r\n

```
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n
```

Query status of the digital output

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
```

If no parameter is specified, all the status of digital output will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1

```
Request:
http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do1=1\r\n
```

Capture single snapshot

Note: This request require normal user privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>]
```

If the user requests the size larger than all stream setting on the server, this request will failed!

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	the channel number of video source
resolution	*<available resolution>*	0	The resolution of image
quality	*1~5*	3	The quality of image

Server will return the most up-to-date snapshot of selected channel and stream in JPEG format. The size and quality of image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

Account management

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]
[&privilege=<value>][…][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	add	Add an account to server. When using this method, “username” field is necessary. It will use default value of other fields if not specified.
	delete	Remove an account from server. When using this method, “username” field is necessary, and others are ignored.

	edit	Modify the account password and privilege. When using this method, “username” field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit
userpass	<value>	The password of new user to add or that of old user to modify. The default value is an empty string.
privilege	<value>	The privilege of user to add or to modify.
	viewer	viewer’s privilege
	operator	operator’s privilege
	admin	administrator’s privilege
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

System logs

Note: This request require administrator privilege

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/syslog.cgi

Server will return the up-to-date system log.

Return:

HTTP/1.0 200 OK\r\n Content-Type: text/plain\r\n Content-Length: <syslog length>\r\n \r\n <system log information>\r\n

Upgrade firmware

Note: This request requires administrator privilege

Method: POST

Syntax:

http://<*servername*>/cgi-bin/admin/upgrade.cgi

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
```

Server will accept the upload file named <file name> to be upgraded the firmware and return with <return page> if indicated.

IP filtering

Note: This request requires administrator access privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<ipaddress>&end=<ipaddress>][&index=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
Method	addallow	Add a set of allow IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	adddeny	Add a set of deny IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	deleteallow	Remove a set of allow IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove a set of deny IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The start IP address to add or to delete.
end	<ip address>	The end IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or

		relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

RTSP SDP

Note: This request requires viewer access privilege

Method: GET/POST

Syntax:

http://<*servername*>/viewer/<0~(n-1)>/<network_accessname_<0~(m-1)>>

rtsp://<*servername*>/<0~(n-1)>/<network_accessname_<0~(m-1)>>

“n” is the channel number and “m” is the stream number.

You can get the SDP by HTTP or just describe by RTSP protocol directly. For detailed streaming protocol, please refer to “control signaling” and “data format” documents.

D. Fiche technique

Video
Compression: MPEG-4 & MJPEG
Resolution max.: 640x480 Pixel
Resolutions posible 640x480, 320x240, 176x144
Taux d'image: max. 25 Images/Seconde

Audio
GSM-AMR, Bitrate: 4.75 Kbit/s
MPEG-4 AAC, Bitrate: 16 Kbit/s à 128 Kbit/s
Audio bidirectionelle
Microphone integre
Entre microphone externe
Sortie audio
Enclenchement muet (Mute)

Streaming
Dualstreaming de MPEG-4 et MJPEG
MPEG-4 Streaming en UDP, TCP ou http
MPEG-4 Multicast Streaming
MPEG-4 Streaming en RTSP
MJPEG Streaming en HHTP

Image settings
Dimension d'image, qualité d'image, taux d'image, temple de temps et titre vidéo dans l'image, vidéo incliner et miroirs, luminosité, contraste, saturation
AGC, AWB, AEC, configuration IR-filtre : auto, manuellement, calendrier, entrée numérique (seulement TV7222, TV7223) Compensation contre lumière (BLC), Masquage de zone privé (5 secteurs, librement définissable)

System
Flash: 8MB
RAM: 64 MB
Processor: ¼ Inch Progressive Scan CCD Sensor
Shutter: 1/30 S. jusqu'a 1/50000 S.
LED. Led en 2 couleurs pour affichage du statut
Filtre IR pour fonction J/N (seulement en TV7222/TV7223)

Reseau
10/100 Mbps Ethernet, RJ-45
Protocols (u.a.): IPv4,TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, und PPPoE
W-LAN 802.11b/g (nur TV7222/TV7223)

Securité
Protection de mot de passe avec plusieurs niveaux
Filtre d'adresses IP
W-LAN: WEP, WPA-PSK, WPA2

Gestion d'événement
Reconnaissance de mouvement vidéo Entrée de distribution et sortie de distribution Information d'événement sur HTTP, SMTP, FTP
enregistrements locale sur un PC en fichè MP4

Allimentation
12VDC / max. 750 mA
802.3af POE (Power over Ethernet) (seulement TV7220, TV7222)

Environs
Temperature: 0~35°C
Humidité: 20%~80% sans condence

Systèmes
OS: Windows XP/2003/Vista
Browser: Internet Explorer, Mozilla Firefox
Mobilw: 3GPP-Player
Real Player 10.5
Quicktime 6.5
Packet Video Player 3.0
VLC Player

E. Indication de licence

GNU GPL

Par la présente indication nous vous informons que la caméra de surveillance réseau TV7220, TV7221, TV7222 et TV7223 comporte des logiciels programmés sous Linux. Pour l'utilisation de ces logiciels, une licence exclusive sous le GNU General Public licence (GPL) doit être accordée. Pour assurer une utilisation GPL conforme, nous vous adressons les conditions de la licence.

Texte de la licence:

Le texte de licence du GNU General Public Licence est enregistré sur le CD ci-joint sous le fichier : CDROM:\GNU_GPL\GPL-Licence.txt ou sur le site internet Security-center sous : http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL

Source Code

Die verwendeten Sourcecodes sind auf der ABUS Securtiy-Center Homepage unter http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL zum kostenfreien Download bereitgestellt.

Fonctionnement du système entier

Les paquets de logiciel (SourceCodes) offerts à téléchargés ne garantissent pas le fonctionnement parfais du système entier. Pour cela il manque plusieurs applications de logiciel et l'équipement informatique convenant aux caméras réseau.

Indication de licence

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:
TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.